Français | Mode d'emploi

IPC-765VGA

CAMERA IP D'INTÉREUR

avec QR-Code / VGA / WiFi / Infrarouge

PX-3722-675

IPC-765VGA

CAMERA IP D'INTÉREUR

avec QR-Code / VGA / WiFi / Infrarouge

© 07/2013 – HA//FD//FrG – GS

TABLE DES MATIÈRES

INTRODUCTION

Votre nouvelle caméra IP 6

Utilisation de cette notice 7

Consignes préalables 9
Consignes de sécurité 9
Informations concernant le recyclage des appareils électriques et électroniques. 10
Déclaration de conformité. 10

Informations produit 11
Contenu 11
Caractéristiques techniques 11
Configuration système requise 12

Description détaillée 13

GUIDE D'INSTALLATION

Installation 15
Recommandations de produits 15
Préparation 16
Branchement et mise en service 18

Accès à la caméra via un navigateur 25

Activer les éléments de contrôle ActiveX 27
Sous Windows 7 (et Vista) 27
Sous Windows XP 35
Restaurer les paramètres par défaut 44

Paramètres Wi-Fi 47

Configurer la connexion 48
WEP 52
WPA et WPA2 53
Connecter 54

Montage 55

UTILISATION

Commandes de base **56**

Définir le mot de passe **57**

Configurer les comptes utilisateurs **59**

Paramètres Wi-Fi **62**

Connecter plusieurs caméras au réseau **64**

Installer les mises à jour **68**

ANNEXE

Branchement de détecteurs de mouvement **73**
- Configuration des alarmes 73
- Broches I/O (Pins) 74
- Activer l'entrée alarme 75
- Connexion I/O en cas d'alarme 76

Dépannage **77**

Notions de base à propos des réseaux **79**
- Matériel 79
- Termes réseau de base 80
- Services réseau 84

Mesures de sécurité dans les réseaux Wi-Fi **88**

Contrat de Licence de Logiciel Libre CeCill **90**

INTRODUCTION

VOTRE NOUVELLE CAMÉRA IP

Chère cliente, cher client,
Nous vous remercions pour l'achat de cette caméra IP Wi-Fi, une puissante caméra réseau qui offre des images de haute qualité consultables via Internet.
Afin d'utiliser au mieux votre nouveau produit, veuillez respecter les consignes et astuces suivantes.

UTILISATION DE CETTE NOTICE

Symboles utilisés

	Ce symbole signale les dangers possibles et les informations importantes sur l'utilisation du produit. Il est utilisé chaque fois que votre attention est particulièrement nécessaire.
	Ce symbole indique les conseils et les informations utiles pour une utilisation optimale du produit.
	Ce symbole est utilisé pour des exemples et des explications qui illustrent des procédures souvent complexes, afin de les rendre plus compréhensibles.
	Ce symbole se trouve derrière les termes techniques expliqués dans le glossaire. Le glossaire aide à la compréhension des termes techniques dans leur contexte.

Mises en forme du texte utilisées

MAJUSCULES	Les majuscules sont utilisées pour nommer des touches, des branchements ou autres composants du produit.
Caractères gras	Les caractères gras sont utilisés pour reconnaître des éléments du menu ou du logiciel.
1. Énumérations 2. Énumérations 3. Énumérations	Les énumérations sont utilisées chaque fois que l'utilisateur doit suivre plusieurs étapes, ou pour présenter les caractéristiques du produit.

Structure

Ce mode d'emploi est divisé en quatre grandes parties :

Chapitre 1 : Introduction	Vous trouverez ici des notes sur l'utilisation de ce guide, des consignes de sécurité importantes concernant le produit, et un aperçu du produit.
Chapitre 2 : Installation	Notice détaillée pour l'installation et la mise en route de la caméra IP et pour la configuration de base.
Chapitre 3 : Utilisation	Consignes de commande et réglages avancés de la caméra IP
Annexe	Dépannage, glossaire, et déclaration de conformité

CONSIGNES PRÉALABLES

Consignes de sécurité

- Ce mode d'emploi vous permet de vous familiariser avec le fonctionnement du produit. Conservez-le afin de pouvoir le consulter en cas de besoin.
- Concernant les conditions de garantie, veuillez contacter votre revendeur. Veuillez également tenir compte des conditions générales de vente !
- Veillez à utiliser le produit uniquement comme indiqué dans la notice. Une mauvaise utilisation peut endommager le produit ou son environnement.
- Le démontage ou la modification du produit affecte sa sécurité. Attention, risque de blessure !
- Ne démontez pas l'appareil, sous peine de perdre toute garantie. Ne tentez jamais de réparer vous-même le produit !
- Manipulez le produit avec précaution. Un coup, un choc, ou une chute, même de faible hauteur, peuvent l'endommager.
- N'exposez pas le produit à l'humidité ni à une chaleur extrême.
- Ne plongez jamais le produit dans l'eau ni dans aucun autre liquide.

ATTENTION :
Le fabricant décline toute responsabilité en cas de dégâts dus à une mauvaise utilisation. Sous réserve de modification et d'erreur !

Informations concernant le recyclage des appareils électriques et électroniques

Votre nouveau produit a été développé avec le plus grand soin et avec des composants de haute qualité. Il devra cependant être un jour recyclé. Le symbole de la poubelle barrée signifie que votre produit devra être recyclé séparément des ordures ménagères à la fin de sa durée de vie. À l'avenir, veuillez amener tous les appareils électriques ou électroniques aux points de ramassage publics de votre municipalité. Ceux-ci prennent en charge vos déchets pour un recyclage écologique et conforme à la législation. Vous évitez ainsi les conséquences négatives sur l'homme et l'environnement pouvant découler d'une mauvaise prise en charge des produits à la fin de leur durée de vie. Les détails concernant la collecte des déchets sont disponibles dans votre municipalité.

Déclaration de conformité

La société Pearl Agency déclare ce produit PX3722 conforme à la directive 1999/5/EG du Parlement Européen concernant les équipements hertziens et les équipements terminaux de télécommunication.

Pearl Agency
Pearl-Str. 1-3
79426 Buggingen
Allemagne
12.07.2013

Le formulaire de conformité détaillé est disponible sur www.pearl.de. Sur le côté gauche de la page, cliquez sur **Support (FAQ, Treiber & Co.)**. Saisissez dans le champ de recherche la référence de l'article, PX3722.

Importé par :
PEARL Diffusion
6, rue de la Scheer
F - 67600 SÉLESTAT

INFORMATIONS PRODUIT

La caméra IP offre une large gamme d'applications aux utilisateurs privés et professionnels.
Pour une protection optimale, elle embarque les normes de sécurité actuelles que sont les cryptages WPA et WPA2. Avec le standard 802.11b/g, vous atteignez des vitesses de transfert de données jusqu'à 54 Mbps. L'antenne externe permet un transfert de données à faibles pertes sur de longues distances. Dans des conditions normales, la caméra peut fonctionner dans toute la zone de couverture de votre routeur Wi-Fi. Pour la surveillance à distance, la caméra peut envoyer des prises de vue et des vidéos par e-mail, ou même les charger sur un serveur FTP configuré. Vous pouvez aussi y accéder à l'aide de votre iPhone.

Contenu
- Caméra IP
- Antenne Wi-Fi
- Câble réseau (RJ45)
- Adaptateur secteur
- CD logiciel
- Mode d'emploi

Caractéristiques techniques
- Capteur CMOS 1/4" (couleur)
- Résolution : 640 x 480 pixels (VGA)
- Vision nocturne grâce à 10 LED IR : portée jusqu'à 10 m
- Sensibilité : 0,5 Lux
- Champ de vision : 280° horizontalement, 90° verticalement
- Taux de fréquence d'image : max. 30 ips (images/sec.)
- Détection de mouvement avec envoi automatique de photo par e-mail
- Microphone intégré
- Supporte de nombreux protocoles Internet et de connexion : HTTP, FTP, TCP/IP, SMTP, DHCP, UDP, UPnP, DDNS, PPoE etc.
- Wi-Fi : Vitesse de transfert jusqu'à 54 Mbits/s(IEEE 802.11g) avec cryptage WEP/ WPA/ WPA2
- Serveur web intégré
- Dimensions : 100 x 125 mm

Configuration système requise

- **Réseau**
  - LAN : Ethernet 10Base-T ou Fast Ethernet 100Base-TX
  - Wi-Fi : IEEE 802.11 b/g

- **Ordinateur pour accès via navigateur web**
  - Système d'exploitation requis : Windows 2000/XP/Vista/7
  - Mémoire vive : 128 Mo RAM
  - Résolution : 800 x 600 ou plus
  - Navigateur : Microsoft Internet Explorer (8.0 ou version ultérieure)
  - Processeur : Intel Pentium III 800 MHz ou supérieur

Caméras brnchées	Processeur	Mémoire
1	Pentium III / 800 MHz	512 MB RAM
2 à 4	Pentium 4 / 1,3 GHz	512 MB RAM
5 à 8	Pentium 4 / 2,4 GHz	1 GB RAM
9 à 16	Pentium 4 / 3,4 GHz	2 GB RAM

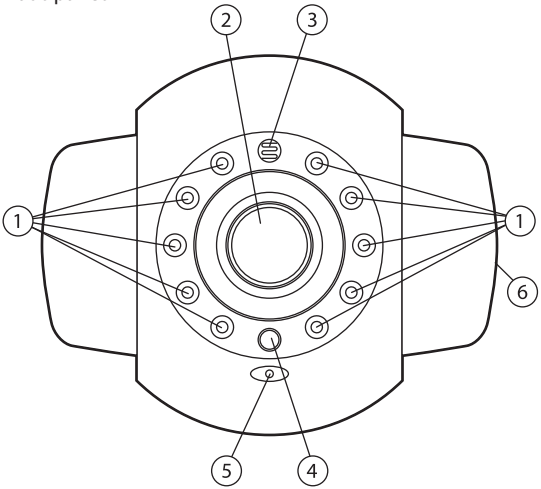
Vous pouvez aussi utiliser des processeurs AMD d'une puissance équivalente. Les données fournies sont des valeurs minimales. Une machine plus puissante facilitera laprise en main.

NOTE :
Le logiciel de la caméra utilise des éléments de contrôle ActiveX. Ainsi, veuillez uniquement utiliser le navigateur Internet Explorer et aucun autre navigateur tel que Mozilla Firefow, Apple Safari ou Google Chrome.

DESCRIPTION DÉTAILLÉE

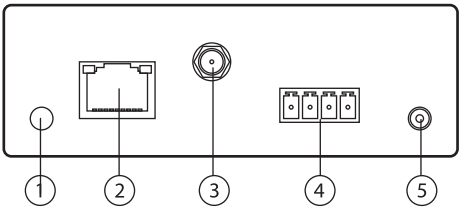
Face avant

1. LED infrarouges
2. Lentille (capteur CMOS avec lentille intégrée)
3. Capteur de luminosité
4. LED réseau
5. Microphone
6. Haut-parleur



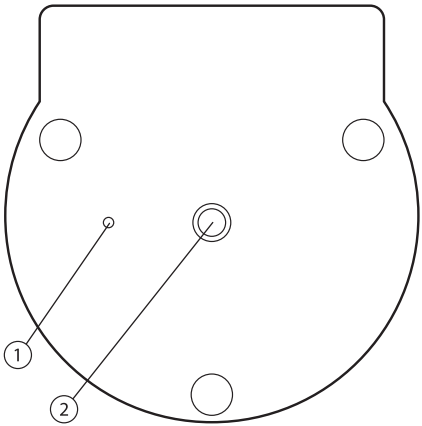
Face arrière

1. Sortie casque
2. Port Ethernet RJ45
3. Antenne
4. Ports alarme I/O
5. Prise pour alimentation secteur



Dessous

1. Touche Reset (réinitialisation)
2. Logement pour support



GUIDE D'INSTALLATION

INSTALLATION

ATTENTION :
Avant d'installer la caméra définitivement, mettez-la en marche et assurez-vous que les deux fonctions LAN et Wi-Fi fonctionnent correctement. Trouvez plus d'informations sur l'installation à la fin de ce chapitre.

NOTE :
La plupart des termes sont expliqués dans l'annexe „Notions de base du réseau". Si toutefois vous avez des questions concernant l'installation, vous pouvez contacter votre revendeur.

Préparation

NOTE :
Si vous n'êtes pas sûr de vos réponses aux questions suivantes, nous vous encourageons à contacter un professionnel. Une mauvaise configuration de la caméra peut y empêcher l'accès.

Pour assurer une bonne installation de la caméra, vous devez rechercher et disposer des informations suivantes à l'avance :

- Les données d'accès de votre fournisseur d'accès à Internet (FAI).
- L'adresse IP de votre routeur / passerelle.
- Le type de réseau (infrastructure ou Adhoc).
- Est-ce qu'un serveur DHCP est déjà utilisé dans votre réseau ? Si oui - quelle plage d'adresse couvre-t-il ?

Vous devriez également considérer les points suivants à l'avance :

- Pour la configuration initiale, la caméra doit être connectée directement au routeur par câble.
- Éloignez toutes les éventuelles sources d'interférence à proximité du routeur sans fil. Cela inclut les téléphones portables, caméras de surveillance sans fil, et autres appareils qui fonctionnent sur la bande des 2,4 GHz.
- Connectez la caméra et le routeur avec un câble de moins de 25 m - dans des conditions défavorables, cela pourrait provoquer une chute de tension et la caméra ne pourrait plus transférer de signal.
- Lors de la connexion de la caméra sur un réseau existant, désactivez tous les pare-feux, antivirus, filtres d'adresses MAC et cryptages de votre routeur.
- Notez sur une feuille le SSID de votre réseau Wi-Fi existant.

NOTE :
Vous trouverez à la fin de ce guide d'installation une liste de contrôle pour l'installation et la mise en service. Découpez cette liste du guide d'installation et utilisez-la pour configurer les différents points.

Branchement et mise en service

ATTENTION :
Respectez obligatoirement l'ordre des prochaines étapes.

1. Utilisez le câble réseau pour brancher la caméra à un port Ethernet libre de votre routeur ou à un switch réseau qui est branché au routeur. Branchez ensuite l'adaptateur secteur au réseau électrique puis au port d'alimentation de la caméra IP.

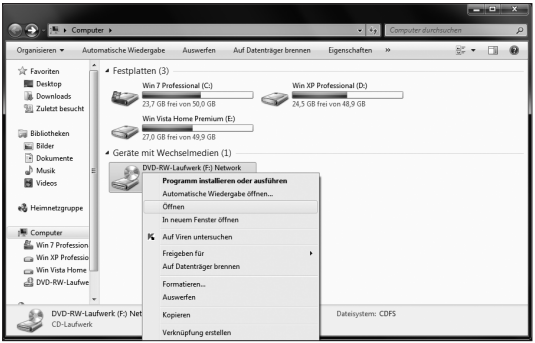
NOTE :
Il est recommandé de brancher l'adaptateur secteur uniquement sur une multiprise disposant d'une protection intégrée contre les surtensions.

2. Démarrez votre ordinateur et installez le logiciel pour accéder à la caméra.
3. Insérez le CD logiciel fourni dans un lecteur CD/DVD de votre ordinateur.

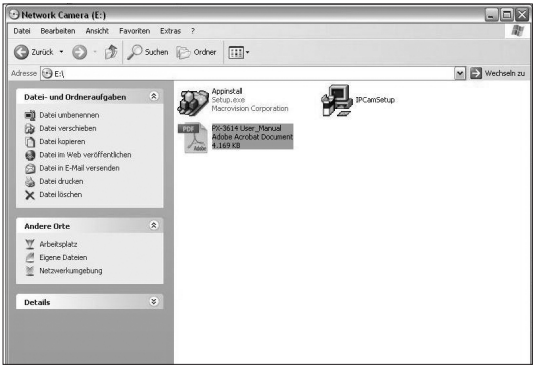
4. Sélectionnez **Exécuter autorun.exe** après que Windows a reconnu le CD. Allez ensuite à l'étape 5.

Automatische Wiedergabe
DVD-RW-Laufwerk (F:) Network Camera
Immer für Software und Spiele durchführen:
Programm installieren oder ausführen
autorun.exe ausführen
Kein Herausgeber angegeben
Allgemeine Optionen
Ordner öffnen, um Dateien anzuzeigen
mit Windows-Explorer
Weitere Optionen für die automatische Wiedergabe in der Systemsteuerung anzeigen

Si le CD ne démarre pas automatiquement, ouvrez le **Poste de travail/Ordinateur** et sélectionnez le lecteur avec un clic droit.



Sélectionnez **Explorer/Ouvrir** pour afficher le contenu du CD.



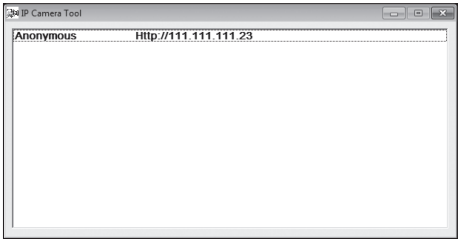
Démarrez l'application **IPCamSetup**.

Welcome
Welcome to the IP Camera Setup program. This program will install IP Camera on your computer.
It is strongly recommended that you exit all Windows programs before running this Setup program.
Click Cancel to quit Setup and then close any programs you have running. Click Next to continue with the Setup program.
WARNING: This program is protected by copyright law and international treaties.
Unauthorized reproduction or distribution of this program, or any portion of it, may result in severe civil and criminal penalties, and will be prosecuted to the maximum extent possible under law.
< Back
Next >
Cancel

Suivez les instructions de l'assistant d'installation. Cliquez sur **Next** (Suivant). Attendez ensuite que l'installation se termine puis cliquez sur **Finish** (Terminer)

5. Démarrez le logiciel en double cliquant sur la nouvelle icône apparue sur le bureau.

Par défaut, la caméra se voit assigner une adresse par DHCP . La fenêtre „IPFinder" affiche les caméras branchées ainsi que leurs IP et adresses MAC .



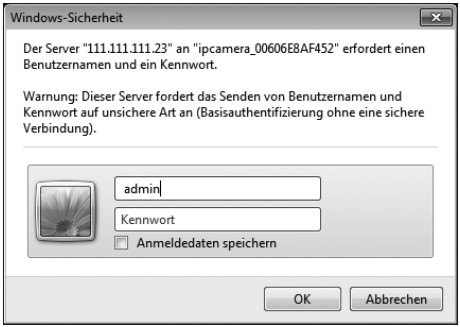
Démarrez Internet Explorer.

NOTE :
Si vous utilisez Microsoft Internet Explorer, vous devez ensuite installer des contrôles Active-X. Veuillez vous référer aux instructions du chapitre suivant. D'autres navigateurs , par exemple Mozilla Firefox, ne peuvent pas afficher les contrôles ActiveX requis et affichent seulement un menu de caméra aux fonctions restreintes. Veuillez vous référer à la section „Utiliser un autre navigateur".

Saisissez l'adresse IP dans la ligne d'adresse de votre navigateur.

EXEMPLE :
Si la caméra est affichée sous l'adresse IP „168.198.0.10", vous devez saisir ces chiffres dans Internet Explorer sous la forme „http://168.198.0.10".

La fenêtre suivante vous demandera votre mot de passe. Saisissez **admin** dans la ligne du dessus. Laissez la seconde ligne vide et cliquez sur **OK**.


Windows-Sicherheit
Der Server "111.111.111.23" an "ipcamera_00606E8AF452" erfordert einen Benutzernamen und ein Kennwort.
Warnung: Dieser Server fordert das Senden von Benutzernamen und Kennwort auf unsichere Art an (Basisauthentifizierung ohne eine sichere Verbindung).
admin
Kennwort
Anmeldedaten speichern
OK
Abbrechen

Le navigateur affiche maintenant l'interface de contrôle en ligne de la caméra IP. La caméra peut maintenant être contrôlée via le navigateur depuis n'importe quel ordinateur connecté à votre réseau.

English 簡体中文 繁體中文 España 한국어 Deutsch Français
ActiveX Mode (For IE Browser)
Sign in
Server Push Mode (For Safari,FireFox, Google Browser)
Sign in
Sign in mobile phone
attention:
case sensitive
propose using 1024 * 768 screen resolution

ATTENTION :
La caméra ne s'affiche pas sous Windows XP avant d'avoir installé les contrôles nécessaires. Seul le message suivant s'affiche : Cette page ne peut pas être affichée. Respectez les étapes du paragraphe „Accès avec Windows XP" (voir page 35) et suivez-les pour réussir à afficher la caméra et vérifier qu'elle soit accessible via cette adresse IP.

Respectez les consignes de la section suivante pour accéder à la caméra. Vous pouvez ensuite configurer les paramètres Wi-Fi et tester les fonctions de base.

ACCÈS À LA CAMÉRA VIA UN NAVIGATEUR

NOTE :
Veuillez suivre les étapes suivantes en mode administrateur pour Internet Explorer.

Vous pouvez utiliser les navigateurs suivants pour accéder à la caméra.

Fournisseur	Navigateur
Microsoft	Internet Explorer
Google	Chrome
Mozilla	Firefox
Macintosh	Safari

Choisissez d'abord la langue voulue dans la première ligne, par exemple **Français**.

Sur l'écran de démarrage de la caméra, vous pouvez choisir d'utiliser Internet Explorer ou un autre navigateur (Mode Server Push).

Cliquez ensuite sur **Inscription** sous **Mode ActiveX** ou **Mode Server Push** selon que vous utilisiez Internet Explorer ou un autre navigateur.

ATTENTION :
Le Mode Server Push ne propose pas toutes les fonctions de la caméra IP. Il ne propose qu'une interface restreinte comme indiqué ici.

NOTE :
*Pour utiliser Microsoft Internet Explorer, il est nécessaire de procéder à des réglages supplémentaires. Veuillez vous référer aux instructions ci-dessous. Si vous utilisez un autre navigateur et avez sélectionné le **Mode Server Push**, sautez le prochain paragraphe et allez à la section „Paramètres Wi-Fi" (voir page 47).*

ACTIVER LES ÉLÉMENTS DE CONTRÔLE ACTIVEX

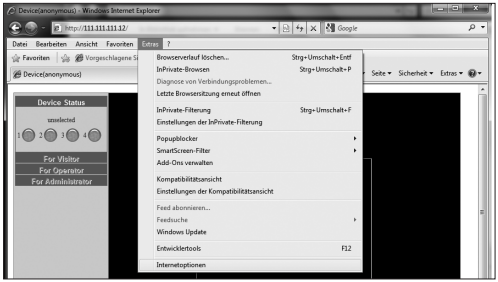
Si vous utilisez Microsoft Internet Explorer et avez choisis le **Mode ActiveX**, vous devez effectuer quelques réglages avant de continuer l'utilisation. Le paragraphe suivant décrit le processus pour Windows 7 et Windows Vista. Si vous utilisez Windows XP, continuez avec le paragraphe „Sous Windows XP" (voir page 35).

Sous Windows 7 (et Vista)

- **Désactiver les paramètres de sécurité**

NOTE :
L'utilisation de la caméra nécessite l'installation d'éléments de contrôle ActiveX sur votre ordinateur. Cela peut être effectué uniquement lorsque les paramètres de sécurité d'Internet Explorer sont désactivés pendant la durée de l'installation. Les paramètres de sécurité seront rétablis dans la dernière section de ce chapitre, afin de ne pas mettre votre système en danger.

Ouvrez le menu **Outils** de votre Internet Explorer et sélectionnez **Options Internet.**

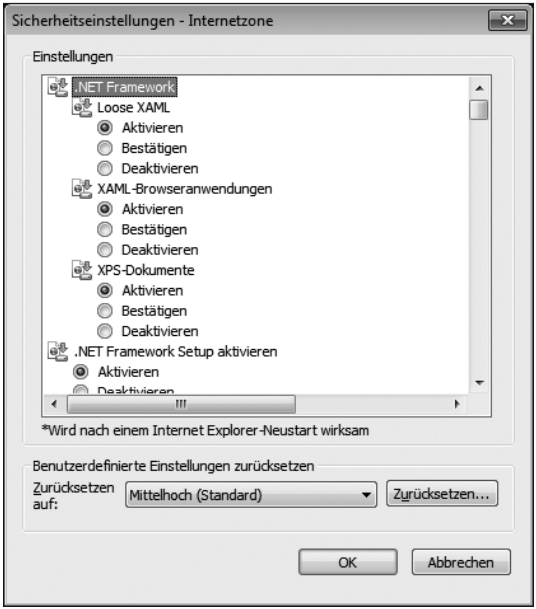


Les options Internet générales apparaissent. Cliquez sur l'onglet **Sécurité**.

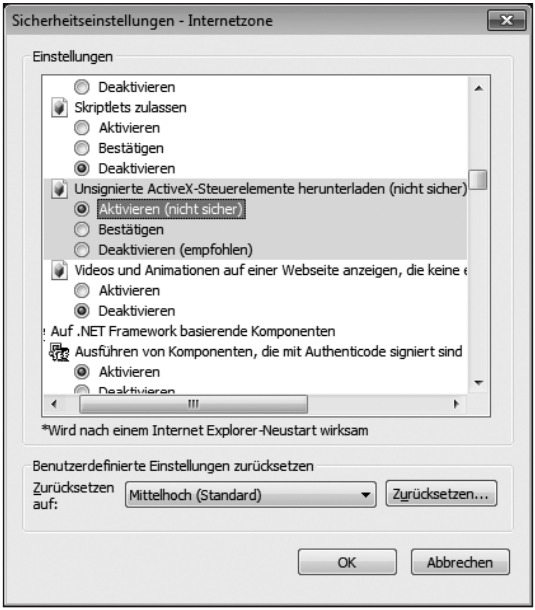
Déplacez la souris dans le cadre **Niveau de sécurité pour cette zone**. Les paramètres de sécurité sont normalement sur **Moyen-haut** ou **Haut**.

Déplacez le curseur vers le bas sur **Moyen** et décochez la case **Activer le mode protégé**.

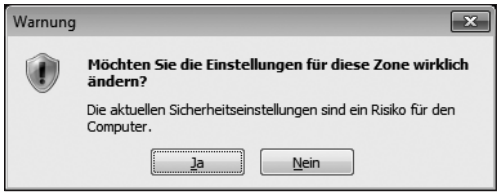
Cliquez sur **Personnaliser le niveau...** pour ouvrir la fenêtre **Paramètres de sécurité – Zone Internet**.



Défilez vers le bas jusqu'au point **Télécharger les contrôles ActiveX non signés**. Sélectionnez **Activé (non sécurisé)** puis cliquez sur **OK**.



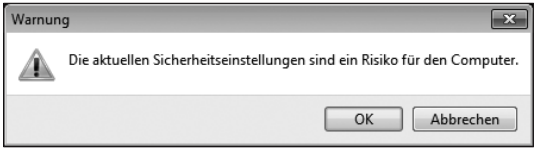
Windows demande confirmation pour modifier les paramètres de sécurité. Cliquez sur **Oui** pour continuer.


Warnung
Möchten Sie die Einstellungen für diese Zone wirklich ändern?
Die aktuellen Sicherheitseinstellungen sind ein Risiko für den Computer.
Ja
Nein

NOTE :
Windows affiche maintenant un message sur les paramètres modifiés. Une nouvelle icône apparaît dans la barre des tâches. Elle vous permet de restaurer facilement les paramètres par la suite. Trouvez plus d'informations dans le chapitre „Restaurer les paramètres de sécurité" (voir page 44).

Cliquez sur **Appliquer**.

Ces paramètres de sécurité ne sont pas recommandés par Windows et une alerte de sécurité vous le rappelle. Cliquez sur **OK** pour continuer.



Les éléments de contrôle requis peuvent maintenant être installés et vous pouvez accéder à la caméra.

- **Accès à la caméra (Windows Vista/7)**
  Saisissez l'adresse IP de la caméra dans la ligne d'adresse d'Internet Explorer. Patientez jusqu'à ce que l'écran de connexion de la caméra se charge.

  Saisissez ensuite votre nom d'utilisateur et mot de passe. Par défaut le nom d'utilisateur est „Admin" et aucun mot de passe n'est défini. Utilisez ces données pour votre premier accès puis cliquez sur **OK**.

Windows-Sicherheit
Der Server "111.111.111.23" an "ipcamera_00606E8AF452" erfordert einen Benutzernamen und ein Kennwort.
Warnung: Dieser Server fordert das Senden von Benutzernamen und Kennwort auf unsichere Art an (Basisauthentifizierung ohne eine sichere Verbindung).
admin
Kennwort
Anmeldedaten speichern
OK
Abbrechen

NOTE :
Une fois connecté, la caméra tente d'installer un élément de contrôle ActiveX. Dans ce cas, l'alerte de sécurité suivante peut s'afficher en haut dans le navigateur : „Voulez-vous autoriser le programme suivant provenant d'un éditeur inconnu à apporter des modifications à cet ordinateur ?". Cliquez sur l'alerte de sécurité et acceptez l'installation. L'écran de connexion est rechargé. Saisissez une nouvelle fois le nom d'utilisateur et le mot de passe (voir ci-dessus) pour accéder à la caméra..

Vous pouvez maintenant tester l'utilisation de base et configurer les paramètres Wi-Fi. Continuez avec „Paramètres Wi-Fi" (voir page 47).

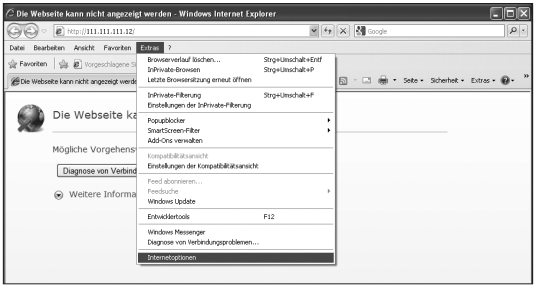
Sous Windows XP

ATTENTION :
L'installation requiert une version récente de Microsoft Internet Explorer. Assurez-vous d'avoir installé toutes les mises à jour disponibles. Vous trouverez des informations complémentaires sur www.microsoft.com.

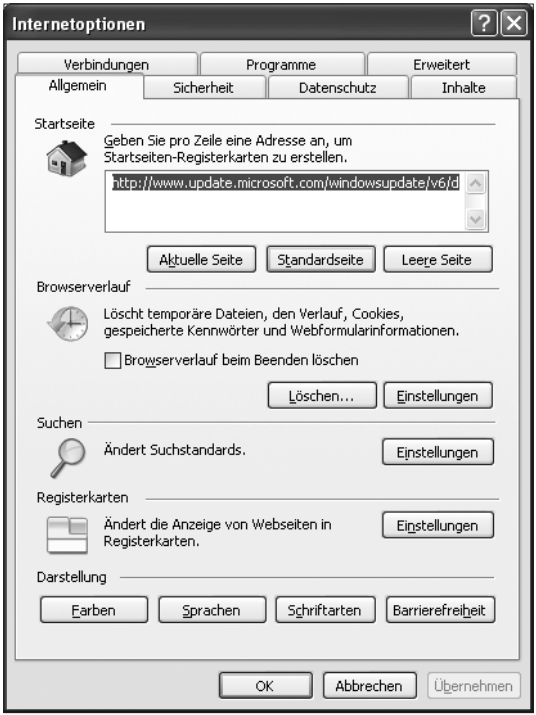
- **Désactiver les paramètres de sécurité**
  L'écran de connexion de la caméra n'apparaît pas avant la fin de l'installation. Même si vous avez saisi l'adresse correcte, le navigateur affiche uniquement le message : **Cette page ne peut pas être affichée**.

NOTE :
L'utilisation de la caméra nécessite l'installation d'éléments de contrôle ActiveX sur votre ordinateur. Cela peut être effectué uniquement lorsque les paramètres de sécurité d'Internet Explorer sont désactivés pendant la durée de l'installation. Les paramètres de sécurité seront rétablis après l'installation, afin de ne pas mettre votre système en danger.

Ouvrez le menu **Outils** de votre Internet Explorer et sélectionnez **Options Internet**.



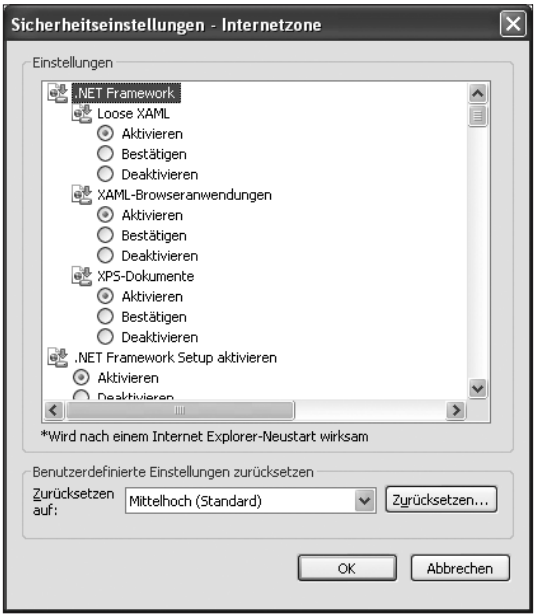
Les options Internet générales apparaissent. Cliquez sur l'onglet **Sécurité**.



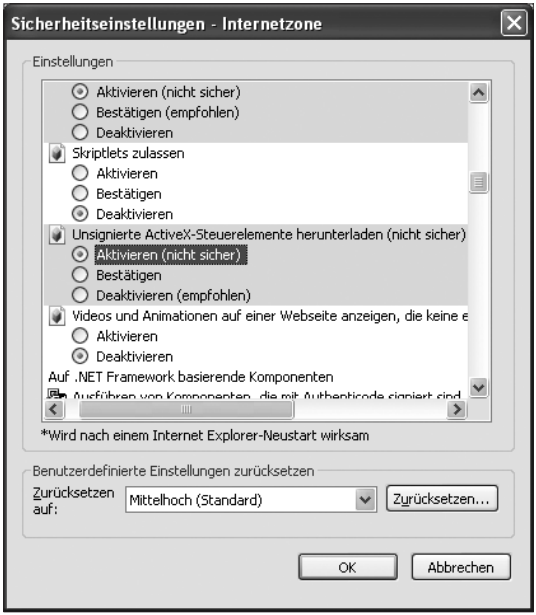
Déplacez la souris dans le cadre **Niveau de sécurité pour cette zone**. Les paramètres de sécurité sont normalement sur **Moyen-haut** ou **Haut**.

Déplacez le curseur vers le bas sur **Moyen**.

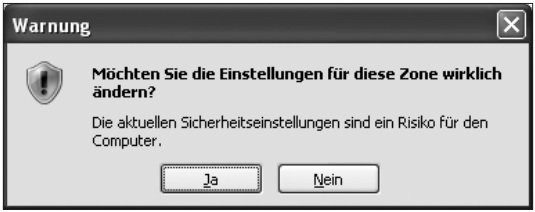
Cliquez sur **Personnaliser le niveau...** pour ouvrir la fenêtre **Paramètres de sécurité – Zone Internet**.



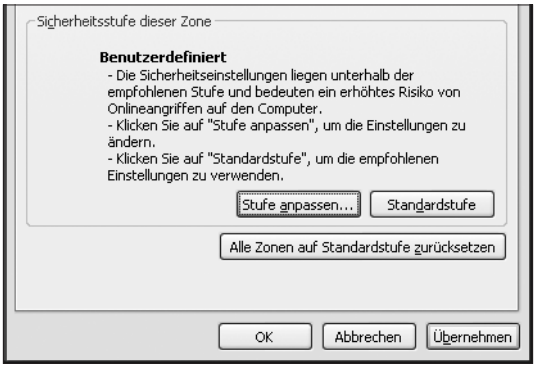
Défilez vers le bas jusqu'aux menus des éléments de contrôle ActiveX. Sélectionnez pour chaque point **Activé (non sécurisé)** puis cliquez sur **OK**.



Windows demande confirmation pour modifier les paramètres de sécurité. Cliquez sur **Oui** pour continuer.


Warnung
Möchten Sie die Einstellungen für diese Zone wirklich ändern?
Die aktuellen Sicherheitseinstellungen sind ein Risiko für den Computer.
Ja
Nein

Cliquez sur **Appliquer**.


Sicherheitsstufe dieser Zone
Benutzerdefiniert
- Die Sicherheitseinstellungen liegen unterhalb der empfohlenen Stufe und bedeuten ein erhöhtes Risiko von Onlineangriffen auf den Computer.
- Klicken Sie auf "Stufe anpassen", um die Einstellungen zu ändern.
- Klicken Sie auf "Standardstufe", um die empfohlenen Einstellungen zu verwenden.
Stufe anpassen...
Standardstufe
Alle Zonen auf Standardstufe zurücksetzen
OK
Abbrechen
Übernehmen

Les éléments de contrôle requis peuvent maintenant être installés et vous pouvez accéder à la caméra.
Saisissez l'adresse IP de la caméra dans la ligne d'adresse d'Internet Explorer. La page de connexion s'affiche.

- **Accès à la caméra (Windows XP)**
  Saisissez l'adresse IP de la caméra dans la ligne d'adresse d'Internet Explorer. La page de connexion de la caméra IP se charge une fois que vous avez désactivé les paramètres de sécurité comme décrit dans la section précédente.

Windows-Sicherheit
Der Server "111.111.111.23" an "ipcamera_00606E8AF452" erfordert einen Benutzernamen und ein Kennwort.
Warnung: Dieser Server fordert das Senden von Benutzernamen und Kennwort auf unsichere Art an (Basisauthentifizierung ohne eine sichere Verbindung).
admin
Kennwort
Anmeldedaten speichern
OK
Abbrechen

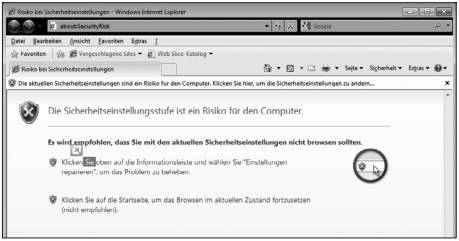
Saisissez ensuite votre nom d'utilisateur et mot de passe. Par défaut le nom d'utilisateur est „Admin" et aucun mot de passe n'est défini. Utilisez ces données pour votre premier accès puis cliquez sur **S'inscrire** sous **Mode ActiveX.**

Vous pouvez maintenant tester l'utilisation de base et configurer les paramètres Wi-Fi. Continuez avec „Paramètres Wi-Fi" (voir page 47).

Restaurer les paramètres par défaut

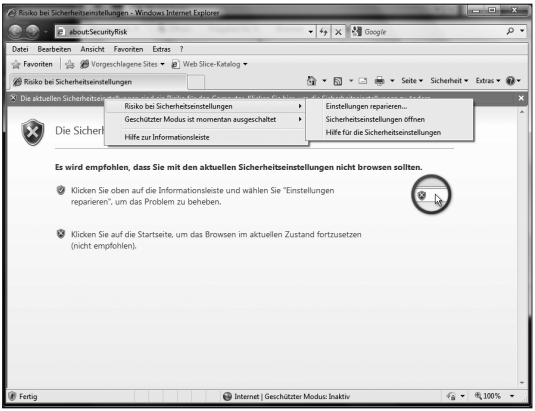
ATTENTION :
Une fois l'installation terminée, vous devez impérativement restaurer les paramètres de sécurité de Microsoft Internet Explorer pour protéger votre système.

Au lancement suivant, Internet Explorer vous avertit que les paramètres de sécurité ne sont pas suffisants.

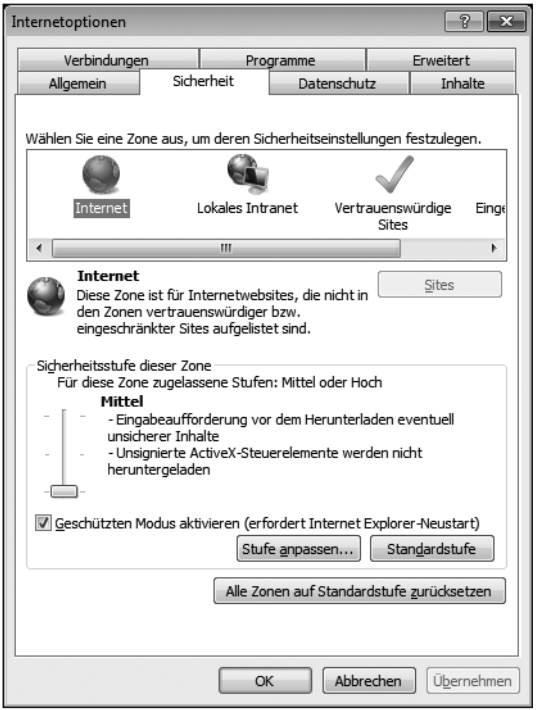

Risiko bei Sicherheitseinstellungen - Windows Internet Explorer
about:SecurityRisk
Datei Bearbeiten Ansicht Favoriten Extras ?
Favoriten
Vorgeschlagene Sites
Web Slice-Katalog
Risiko bei Sicherheitseinstellungen
Seite
Sicherheit
Extras
Die aktuellen Sicherheitseinstellungen sind ein Risiko für den Computer. Klicken Sie hier, um die Sicherheitseinstellungen zu ändern...
Die Sicherheitseinstellungsstufe ist ein Risiko für den Computer.
Es wird empfohlen, dass Sie mit den aktuellen Sicherheitseinstellungen nicht browsen sollten.
Klicken Sie oben auf die Informationsleiste und wählen Sie "Einstellungen reparieren", um das Problem zu beheben.
Klicken Sie auf die Startseite, um das Browsen im aktuellen Zustand fortzusetzen (nicht empfohlen).

Suivez les instructions pour restaurer les paramètres de sécurité.

Cliquez sur le message en haut de la fenêtre du navigateur et choisissez l'onglet **Risque dans les paramètres de sécurité** et **Ouvrir paramètres de sécurité**.


Risiko bei Sicherheitseinstellungen - Windows Internet Explorer
about:SecurityRisk
Datei Bearbeiten Ansicht Favoriten Extras ?
Favoriten
Vorgeschlagene Sites
Web Slice-Katalog
Risiko bei Sicherheitseinstellungen
Seite
Sicherheit
Extras
Risiko bei Sicherheitseinstellungen
Geschützter Modus ist momentan ausgeschaltet
Hilfe zur Informationsleiste
Einstellungen reparieren...
Sicherheitseinstellungen öffnen
Hilfe für die Sicherheitseinstellungen
Es wird empfohlen, dass Sie mit den aktuellen Sicherheitseinstellungen nicht browsen sollten.
Klicken Sie oben auf die Informationsleiste und wählen Sie "Einstellungen reparieren", um das Problem zu beheben.
Klicken Sie auf die Startseite, um das Browsen im aktuellen Zustand fortzusetzen (nicht empfohlen).
Fertig
Internet | Geschützter Modus: Inaktiv
100%

Dans la fenêtre suivante, sélectionnez **Rétablir toutes les zones au niveau par défaut**.



Cliquez sur **Appliquer** pour terminer la procédure.
La caméra peut maintenant être utilisée. Passez au paragraphe „Paramètres Wi-Fi“ (voir page 47) si vous voulez utiliser la caméra sans fil. Allez directement au paragraphe „Commandes de base“ (voir page 55) si vous voulez utiliser la caméra avec un branchement Ethernet.

PARAMÈTRES WI-FI

Vous pouvez ainsi faire fonctionner la caméra via le câble réseau ou la connecter à votre réseau Wi-Fi. Le paragraphe suivant décrit les paramètres Wi-Fi. Si vous souhaitez continuer à utiliser la caméra via le câble, vous pouvez sauter ce paragraphe et passer directement à „Montage“ (voir page 54).

Pour faire fonctionner la caméra via Wi-Fi, vous devez d'abord saisir les données d'accès à votre réseau. Les réglages peuvent être effectués uniquement tant que la caméra est connectée à votre routeur via un câble. Suivez les étapes du paragraphe précédent „Branchement et mise en route“ puis continuez avec le premier point de ce paragraphe.

NOTE :
Assurez-vous que votre routeur n'utilise pas de liste blanche car la caméra ne pourrait pas se connecter au réseau. Si votre réseau utilise une liste blanche, ajoutez-y l'adresse IP de la caméra.

CONFIGURER LA CONNEXION

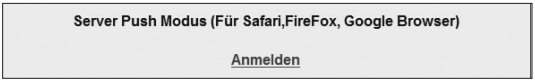
Connectez-vous sur la page d'accueil de la caméra IP comme décrit dans les paragraphes précédents.
Saisissez le nom d'utilisateur „Admin".
Confirmez en cliquant sur OK.

Windows-Sicherheit
Der Server "111.111.111.23" an "ipcamera_00606E8AF452" erfordert einen Benutzernamen und ein Kennwort.
Warnung: Dieser Server fordert das Senden von Benutzernamen und Kennwort auf unsichere Art an (Basisauthentifizierung ohne eine sichere Verbindung).
admin
Kennwort
Anmeldedaten speichern
OK
Abbrechen

Choisissez la langue **Français**.

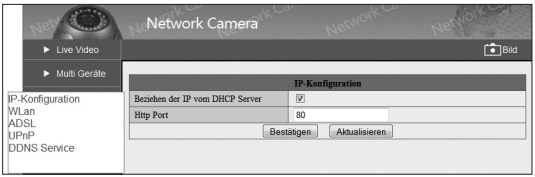
Cliquez sur **Inscription** sous **Mode Active X** si vous utilisez Microsoft Internet Explorer.

Cliquez sur **Inscription** sous **Mode Server Push** si vous utilisez un autre navigateur.



ATTENTION :
Toutes les fonctions de la caméra IP ne sont pas disponibles lors de l'utilisation d'autres navigateurs. L'utilisation de Microsoft Internet Explorer est expressément recommandée.

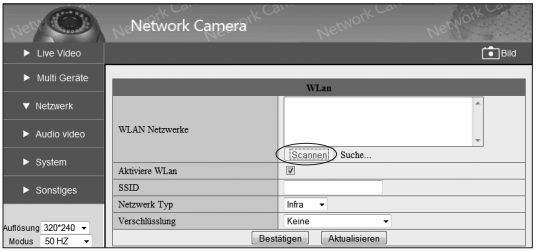
Cliquez sur **Réseau** et sélectionnez **Wi-Fi**.



La page des paramètres réseau est maintenant chargée et le menu des options de l'appareil s'affiche.

Cochez **Activer Wi-Fi** pour ouvrir le menu avancé.

Cliquez sur **Rechercher**. La caméra tente de détecter automatiquement les réseaux Wi-Fi. Vérifiez que votre réseau soit affiché sous **SSID**. Si ce n'est pas le cas, saisissez manuellement votre SSID.



Choisissez un type de réseau **Infra** ou **Adhoc**. **Adhoc** est le bon choix pour la plupart des réseaux domestiques.

Choisissez maintenant le **Cryptage** utilisé par votre réseau. Pour plus d'informations, suivez les instructions du manuel de votre routeur Wi-Fi. Si vous n'utilisez pas de cryptage, cliquez sur **Confirmer** et passez à l'étape „Connecter" (voir page 53).

ATTENTION :
Il est fortement recommandé de sécuriser votre réseau par un cryptage WPA2. Trouvez plus d'informations à ce sujet dans l'annexe.

Si votre réseau utilise un cryptage WEP, suivez les étapes du paragraphe suivant „WEP“ puis continuez avec „Connecter“ (voir page 53).
Si votre réseau utilise le cryptage WPA ou WPA2, suivez les étapes du paragraphe suivant, „WPA et WPA2“ puis continuez avec „Connecter“ (voir page 53).
Cliquez sur **Confirmer** pour enregistrer les paramètres, puis continuez avec le paragraphe „Connecter“ (voir page 53).

Accéder à l'interface web via un iPhone
Vous pouvez également accéder à l'interface web de la caméra via le navigateur Internet de votre iPhone. Pour cela, activez la page d'accueil de la caméra et sélectionnez le lien correspondant. En mode smartphone, seules les fonctions de base de la caméra sont disponibles.

NOTE :
L'interface web de la caméra fonctionne uniquement sur les smartphones qui supportent la transmission vidéo via un réseau.

Connecter la caméra à un iPhone
1. Installez l'application „7links IP Cam Remote“ à partir de App Store.
2. Ouvrez l'application.
3. Appuyez sur „Add Camera“.
4. Appuyez sur „Scan QR-Code“ et scannez ensuite, à l'aide de la fenêtre de numérisation ouverte, le code QR situé en bas de la caméra.
5. Saisissez le mot de passe 000000. Le mot de passe par défaut, préréglé en usine, est 000000. Modifiez le mot de passe pour éviter tout accès non désiré.

NOTE :
Vous pouvez également accéder à la caméra à partir de votre iPhone, via une connexion EDGE, 3G ou Wi-Fi.

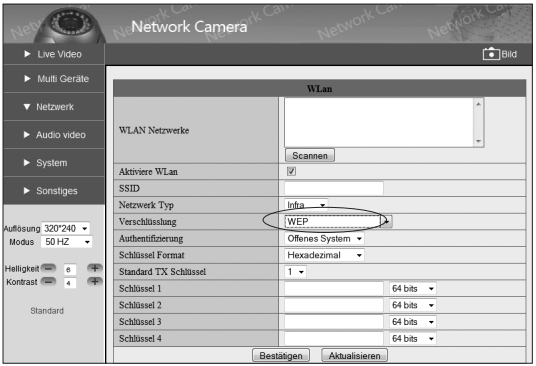
Guide d'installation

- Paramètres P2P

Cliquez sur „Params Settings" „P2P-Settings" afin de modifier les données pour la connexion de votre iPhone.

WEP

Les étapes suivantes permettent d'accéder à la caméra IP sur un réseau crypté WEP .



Sélectionnez d'abord **WEP** dans le menu déroulant pour ouvrir les champs d'informations nécessaires.

Authentifizierung	Offenes System
Sélectionnez sous **Identification** si vous utilisez un système ouvert ou Pre-Shared Key .	

Schlüssel Format	Hexadezimal

Définissez ici si votre clé réseau utilise le système hexadécimal ou les caractères ASCII.

Standard TX Schlüssel	1

Sélectionnez la clé qui utilisée par défaut par votre réseau.

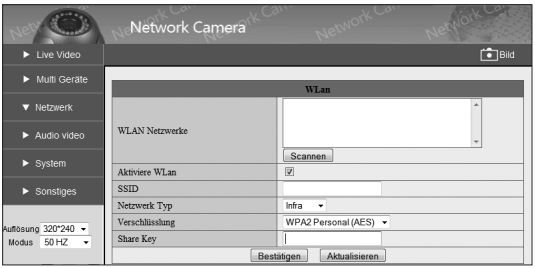
Schlüssel 1		64 bits
Schlüssel 2		64 bits
Schlüssel 3		64 bits
Schlüssel 4		64 bits

Saisissez la Pre Shared Key de votre réseau et indiquez s'il s'agit d'un cryptage 64 ou 128-Bit. Vous devez seulement saisir la clé du point précédent.

Cliquez sur **Confirmer** pour enregistrer les paramètres puis continuez avec le paragraphe „Connecter". La caméra redémarre pour charger les nouveaux paramètres.

WPA et WPA2

Les étapes suivante permettent d'accéder à la caméra IP sur un réseau crypté WPA ou WPA2.



Sélectionnez le type WPA utilisé et saisissez la Pre-Shared-Key. Cliquez sur **Confirmer** pour enregistrer les paramètres puis continuez avec le paragraphe „Connecter“.

Connecter

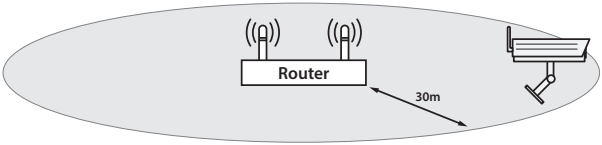
Après avoir effectué les paramètres des sections précédentes, vous pouvez aussi contrôler la caméra IP sans fil. Débranchez le câble Ethernet et vissez l'antenne à l'arrière de la caméra IP. Démarrez ensuite votre navigateur et saisissez à nouveau l'adresse IP de la caméra. La page de connexion de la caméra se charge.

Windows-Sicherheit
Der Server "111.111.111.23" an "ipcamera_00606E8AF452" erfordert einen Benutzernamen und ein Kennwort.
Warnung: Dieser Server fordert das Senden von Benutzernamen und Kennwort auf unsichere Art an (Basisauthentifizierung ohne eine sichere Verbindung).
admin
Kennwort
Anmeldedaten speichern
OK
Abbrechen

Saisissez à nouveau le nom d'utilisateur et le mot de passe. L'accès à la caméra se fait de la même manière que dans les paragraphes précédents „Accès à la caméra via un navigateur“ (voir page 25).

MONTAGE

Vous pouvez installer la caméra IP une fois qu'elle est prête et que le réseau a été détecté. Assurez-vous que la caméra puisse surveiller la zone voulue tout en restant à portée de votre routeur Wi-Fi. La portée maximale pour une connexion W-iFi stable est en moyenne de 30 mètres.



UTILISATION

COMMANDES DE BASE

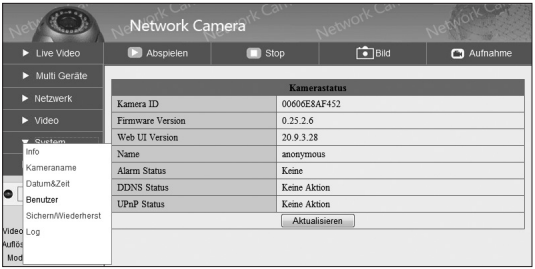
Après la connexion, vous voyez l'image de la caméra et le panneau de contrôle. En tant qu'administrateur, vous pouvez accéder à toutes les fonctionnalités de la caméra.

1. Lecture
2. Stopper la lecture
3. Déclencheur de photo instantanée
4. Démarrer un enregistrement vidéo
5. Affichage vidéo
6. Résolution
7. Mode
8. Luminosité
9. Contraste
10. Restaurer toutes les valeurs de ce menu aux paramètres par défaut
11. Boutons de contrôle
12. Fonction de patrouille

DÉFINIR LE MOT DE PASSE

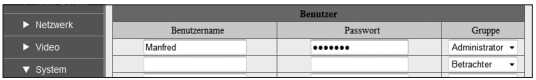
Chaque utilisateur devrait dès le départ définir un nouveau nom d'utilisateur et mot de passe pour protéger la caméra contre les accès non autorisés. Pour cela, suivez les étapes suivantes.

Cliquez sur **Système**.



Dans le menu déroulant, cliquez sur **Utilisateur**.

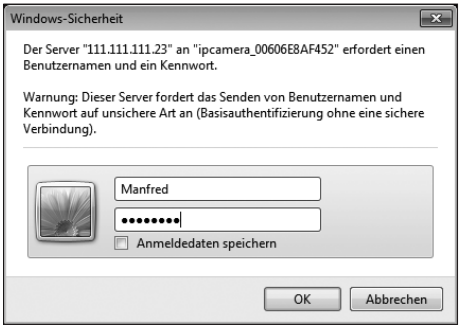
Dans la case du dessus, remplacez „admin" par le nom d'utilisateur voulu.



Saisissez le mot de passe voulu dans la case **Password** (Mot de passe).

Cliquez sur **Confirmer** pour enregistrer les paramètres.

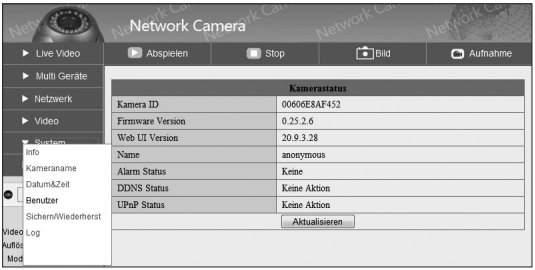
À partir de maintenant, le nom d'utilisateur défini et le mot de passe correspondant seront nécessaires pour accéder à la caméra via la page de connexion.


Windows-Sicherheit
Der Server "111.111.111.23" an "ipcamera_00606E8AF452" erfordert einen Benutzernamen und ein Kennwort.
Warnung: Dieser Server fordert das Senden von Benutzernamen und Kennwort auf unsichere Art an (Basisauthentifizierung ohne eine sichere Verbindung).
Manfred
Anmeldedaten speichern
OK
Abbrechen

CONFIGURER LES COMPTES UTILISATEURS

Vous pouvez créer des comptes utilisateurs pour la caméra IP avec différents droits d'accès.

Cliquez sur **Système**.



Dans le menu déroulant, cliquez sur **Utilisateur**.

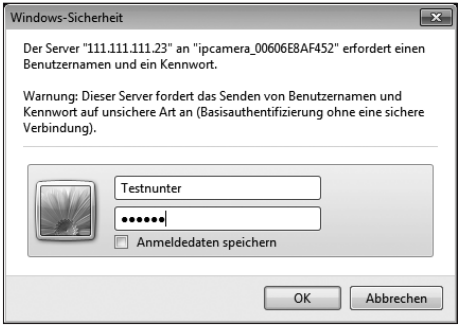
Saisissez le nom d'utilisateur voulu et le mot de passe correspondant.

Sélectionnez dans le menu déroulant les droits d'accès voulus puis cliquez sur **Confirmer**.

Observateur	Peut uniquement regarder l'écran actuel de la caméra.
Utilisateur	Peut démarrer/arrêter l'affichage, prendre des photos et démarrer les enregistrements.
Administrateur	A un accès complet à tous les paramètres de la caméra.

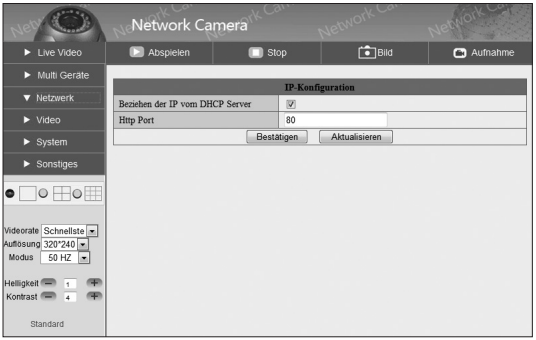
ATTENTION :
En temps normal, seul votre propre compte utilisateur devrait disposer des privilèges d'administrateur.

Le nouvel utilisateur créé peut désormais se connecter à la caméra.

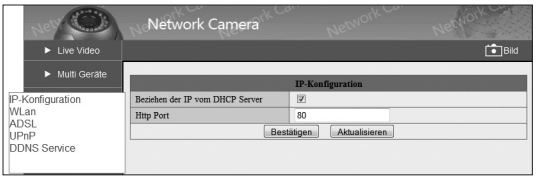

Windows-Sicherheit
Der Server "111.111.111.23" an "ipcamera_00606E8AF452" erfordert einen Benutzernamen und ein Kennwort.
Warnung: Dieser Server fordert das Senden von Benutzernamen und Kennwort auf unsichere Art an (Basisauthentifizierung ohne eine sichere Verbindung).
Testnunter
Anmeldedaten speichern
OK
Abbrechen

PARAMÈTRES WI-FI

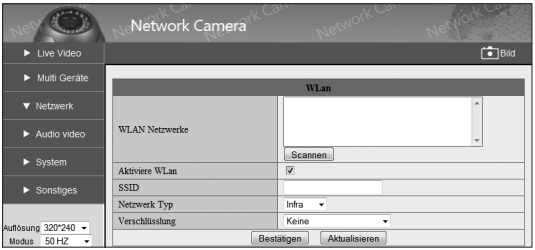
La caméra peut être connectée dans un réseau Wi-Fi existant. Pour cela, elle doit d'abord être connectée au réseau via le câble de sorte à effectuer les réglages nécessaires. Pour accéder aux réglages, cliquez sur **Réseau**.



Cliquez ensuite sur **Wi-Fi**.



Cochez la case **Activer Wi-Fi**.



NOTE :
Comme les paramètres Wi-Fi sont nécessaires à la mise en service de la caméra, ils sont traités en détail dans le chapitre „Installation" (voir page 15).

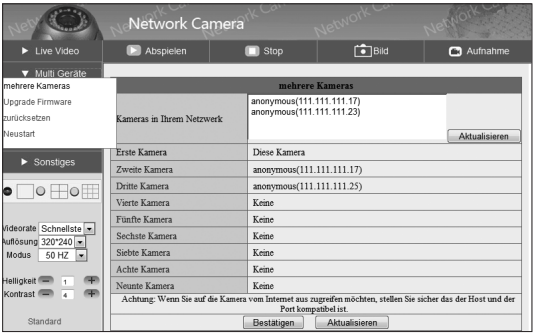
CONNECTER PLUSIEURS CAMÉRAS AU RÉSEAU

Si vous utilisez plusieurs caméras IP de la série PX3722 et PX3723, vous pouvez contrôler jusqu'à 9 caméras via une seule fenêtre de navigateur.

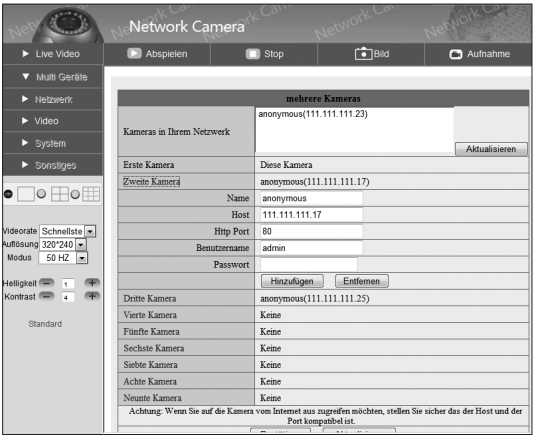
Connectez-vous à la „caméra principale" voulue. La caméra IP choisie n'a pas d'importance. Après configuration, vous devez toujours utiliser la même caméra ou effectuer les réglages suivants pour chaque caméra de votre réseau.

Windows-Sicherheit
Der Server "111.111.111.17" an "ipcamera_00606E7BA6F8" erfordert einen Benutzernamen und ein Kennwort.
Warnung: Dieser Server fordert das Senden von Benutzernamen und Kennwort auf unsichere Art an (Basisauthentifizierung ohne eine sichere Verbindung).
admin
Kennwort
Anmeldedaten speichern
OK
Abbrechen

Cliquez sur **Multi appareils** et sélectionnez l'onglet **Plusieurs caméras**.



Cliquez sur **Deuxième caméra**.



La case **Caméra dans votre réseau** affiche les autres caméras. Double-cliquez sur l'affichage pour copier l'adresse IP dans la case **Host** (Hôte). Si une caméra ne s'affiche pas, vous pouvez également saisir son adresse dans la case **Host**.
Si vous avez assigné un nom à la caméra, saisissez-le sous **Name**. Sinon, ce champ peut rester vide.
Saisissez le **Port http** de la caméra. C'est généralement le port 80 si vous ne l'avez pas changé manuellement.
Saisissez le nom d'utilisateur et le mot de passe du compte administrateur de la caméra cible. Consultez aussi le paragraphe „Configurer le mot de passe" (voir page 56). Cliquez enfin sur **Ajouter**.

NOTE :
Vous aurez besoin du nom d'utilisateur et du mot de passe pour les caméras que vous voulez connecter et non les données de la caméra en cours d'utilisation.

Cliquez sur **Live Video** (Vidéo en direct). La caméra apparaît alors comme point vert supplémentaire sur la barre inférieure.

Si une caméra n'est pas accessible, le cercle est affiché en orange.

Choisissez une des fenêtres mosaïques pour voir les images de toutes les caméras connectées.

Ouvrez le contrôle d'ur

: sur l'image de la caméra. Pour cela, reportez-vous au paragraphe „Commandes de base“ (voir page 55). Avec un double-clic sur l'écran, vous pouvez visionner les images en plein écran.
Répétez ces étapes pour interconnecter jusqu'à 9 caméras au réseau.

NOTE :
Si vous voulez connecter à la fois des caméras extérieures et intérieures, vous devez utiliser le menu de contrôle d'une caméra d'intérieur pour les commandes. Étant donné que les caméras d'intérieur peuvent être déplacées via le navigateur, elles disposent d'un menu plus complet qu'il est préférable d'utiliser pour leur contrôle. Les boutons de commande ne fonctionnent pas avec une caméra IP d'extérieur.

INSTALLER LES MISES À JOUR

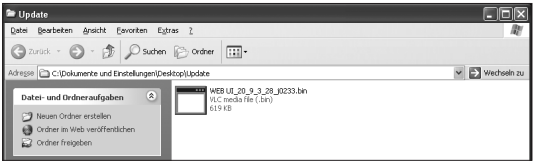
Si de nouvelles versions du firmware sont disponibles, vous les trouverez sur www.pearl.fr. Ces mises à jour servent à étendre les fonctionnalités et à corriger d'éventuels dysfonctionnements.

Veuillez suivre précisément les étapes ci-dessous afin de réussir la mise à jour.

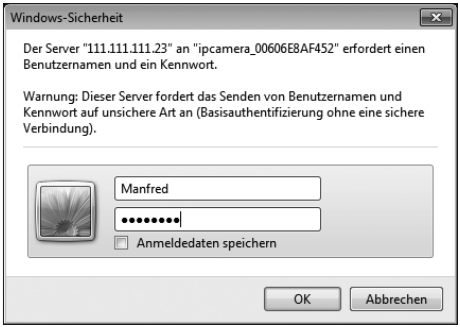
ATTENTION :
L'alimentation de la caméra ne doit pas être coupée durant la mise à jour de la caméra.

Connectez-vous à votre compte client sur le site. Cliquez ensuite sur le bouton „**Notices Patchs Pilotes**", entrez la référence du produit, cliquez sur **OK**, et vous pourrez télécharger les notices, patchs et pilotes des articles que vous avez commandés.

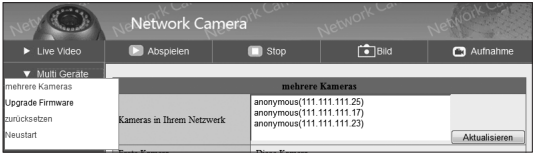
Enregistrez le fichier de mise à jour sur le bureau de votre ordinateur ou dans un nouveau dossier. Il s'agit d'un fichier .bin. Ne modifiez pas le nom du fichier, car la mise à jour ne pourrait pas s'installer.



Démarrez Internet Explorer et saisissez l'adresse IP de votre caméra. Voir les indications du chapitre précédent concernant la saisie. Patientez jusqu'à ce que l'écran de connexion s'affiche.


Windows-Sicherheit
Der Server "111.111.111.23" an "ipcamera_00606E8AF452" erfordert einen Benutzernamen und ein Kennwort.
Warnung: Dieser Server fordert das Senden von Benutzernamen und Kennwort auf unsichere Art an (Basisauthentifizierung ohne eine sichere Verbindung).
Manfred
Anmeldedaten speichern
OK
Abbrechen

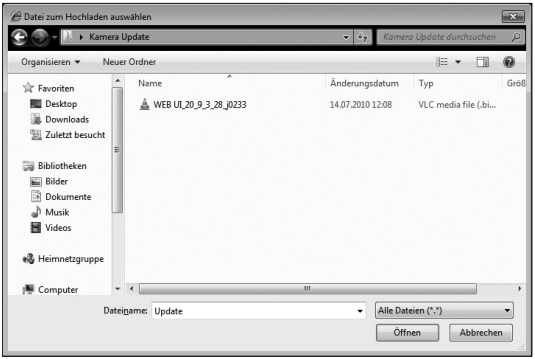
Dans la fenêtre de navigateur de la caméra, sélectionnez **Multi appareils**.



Sélectionnez le point **MAJ Firmware**.

Sélectionnez **Mise à Jour de l'UI web intégré à la caméra** puis cliquez sur **Parcourir.**

Attendez que la fenêtre de sélection du fichier s'ouvre et sélectionnez le fichier de mise à jour. Cliquez sur **Ouvrir**.

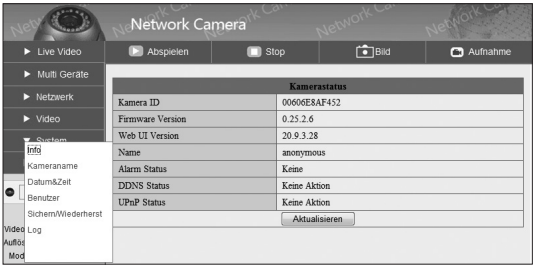


Cliquez sur **Confirmer**.

Le logiciel de la caméra tente maintenant de redémarrer.

Patientez jusqu'à ce que le compte à rebours ait expiré. Redémarrez Internet Explorer et saisissez l'adresse IP de la caméra. Vous serez accueilli par la nouvelle fenêtre de connexion. Saisissez le nom d'utilisateur et le mot de passe habituels.

Le nouveau firmware est maintenant prêt et peut être utilisé. Vous pouvez à tout moment vérifier la version du firmware en cours d'utilisation en cliquant sur **Système** puis sur l'onglet **Info**.



ATTENTION :
La caméra peut être endommagée si elle est déconnectée de l'alimentation ou de votre ordinateur durant le processus de mise à jour. Nous déclinons toute responsabilité et annulons toute garantie en cas de dommages dus à une mise à jour incorrecte. Respectez scrupuleusement les étapes énumérées ici.

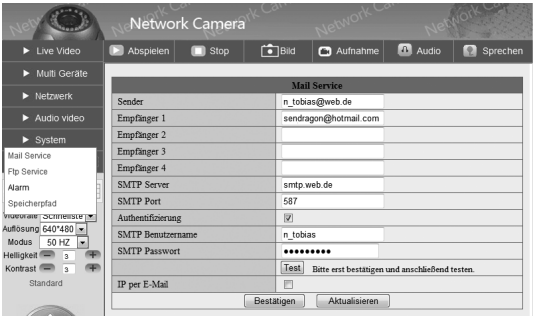
ANNEXE

BRANCHEMENT DE DÉTECTEURS DE MOUVEMENT

Vous pouvez connecter un détecteur de mouvement aux ports I/O situés au dos de la caméra.

Configuration des alarmes

Cliquez sur **Divers** puis sélectionnez **Alarme** pour configurer la fonction détection de mouvement.



Cochez **Détecteur de mouvement activé** pour utiliser la fonction.

Une fois que la détection de mouvement est activée, vous pouvez configurer d'autres paramètres (p.ex. la sensibilité et le type d'alarme).

Broches I/O (Pins)

1. Sortie (+ 5 V)
2. Sortie
3. Entrée alarme
4. Entrée (GND)

Activer l'entrée alarme
Cochez **Entrée alarme activée** pour utiliser la fonction.

EXEMPLE :
Vous pouvez connecter un capteur PIR pour la détection de mouvement. Lorsque le capteur externe s'active, la caméra peut être programmée de sorte à envoyer un e-mail avec une image ou à l'enregistrer dans la mémoire interne.
Si vous connecter une alarme externe avec Pin 3 et Pin 4, l'alarme externe s'active dès que vous avez sélectionné le champ dans **Entrée alarme activée**.

Connexion I/O en cas d'alarme

En cas d'alarme, la connexion I/O s'active. Pin 1 est utilisé en tant que sortie en cas de déclenchement. Pin 2 est utilisé à la fin.

Avec les champs et , vous pouvez contrôler manuellement Pin 1 (+5 V).

NOTE :
Cochez les types de réaction de votre choix après le déclenchement d'une alarme. La caméra peut envoyer des images par e-mail, les enregistrer sur l'ordinateur ou les charger sur un serveur. Les paramètres doivent avoir été préalablement définis dans les différents menus.

DÉPANNAGE

La caméra n'est pas reconnue sur le réseau

1. Vérifiez que l'adresse IP de la caméra soit dans le même sous-réseau que le reste du réseau.
2. . Assurez-vous que l'IP et l'adresse MAC de la caméra ne soient pas déjà affectées à d'autres périphériques de votre réseau.
3. Vérifiez étape par étape, les paramètres réseau de la caméra IP.
4. Assurez-vous que votre routeur accepte les paquets entrants du port 80 .
5. Vérifiez que votre routeur redirige les ports.

J'ai oublié le mot de passe et/ou le nom d'utilisateur

La seule façon de pouvoir accéder à la caméra est de rétablir les paramètres par défaut. La touche Reset se trouve sous la caméra. Utilisez un trombone ou un objet similaire pour appuyer sur ce bouton pendant quelques secondes. La caméra est réinitialisée et peut à nouveau être utilisée avec le nom d'utilisateur „admin" et sans un mot de passe.

ATTENTION :
Restaurer les paramètres par défaut supprimera tous les réglages effectués. Toutes les données des utilisateurs seront perdues, les informations d'accès au réseau effacées et il faudra totalement reconfigurer la caméra IP. Par conséquent, n'effectuez pas cette opération sans réflexion préalable.

Le transfert des images est saccadé et/ou de qualité inférieure

Le transfert est influencée par plusieurs facteurs, dont la bande passante utilisée, le nombre de caméras IP, la puissance du processeur de votre ordinateur, le nombre d'accès, les signaux parasites dans le réseau Wi-Fi (sur la fréquence 2,4 GHz) et les réglages de mode et de luminosité. Vérifiez si l'un de ces facteurs est anormalement élevé ou faible afin d'identifier le problème. Si votre réseau utilise des hubs, remplacez-les par des switchs réseau afin d'assurer une meilleure transmission.

NOTIONS DE BASE À PROPOS DES RÉSEAUX

Ce glossaire vous aide à mieux comprendre certains termes liés aux réseaux. Le paragraphe suivant présente le matériel de base pour un réseau local classique ainsi que les applications et services associés.

Matériel (Hardware)

- **Câble réseau/câble Ethernet**
  Il existe deux variantes : les câbles „droits" et „croisés". Les câbles droits sont le plus souvent utilisés dans les réseaux. Ils permettent la connexion entre ordinateur et switchs, hubs ou routeurs. Les câbles croisés sont utilisés pour connecter directement deux ordinateurs entre eux sans utiliser de réseau. Les câbles droits sont habituellement fournis avec les produits réseau.

- **Modem ADSL**
  Le modem ADSL connecte votre ordinateur à Internet. Si vous voulez avoir accès à Internet sur plusieurs ordinateurs via une ligne, vous devez brancher un routeur directement derrière le modem ADSL.

- **Modem câble**
  Un modem câble est un appareil qui envoie les données via le réseau câblé (télé) et permet une connexion à Internet haut débit via le câble.

- **Point d'accès**
  Le point d'accès ou Access-Point est la „station de base" dans un réseau sans fil (Wi-Fi). Cette fonction est souvent assurée par un routeur dans les réseaux locaux .

- **Routeur**
  Les routeurs permettent la gestion d'accès de tous les ordinateurs du réseau entre eux et avec Internet. Le branchement au routeur peut se faire par câble ou par Wi-Fi selon le modèle. La plupart des routeurs supportent aussi les fonctions DHCP, QoS, Firewall, NTP, etc.

- **Switch réseau**
  Les switchs sont des multiprises réseau. Ils permettent le branchement de plusieurs appareils réseau sur un même câble. Les switchs sont souvent agencés de manière logique, par exemple pour connecter tous les ordinateurs d'un bureau. En couplant plusieurs switchs, on obtient un réseau complexe avec une structure en arborescence.

Termes réseau de base

- **Adresse IP**
  Les adresses IP sont utilisées pour connecter ordinateurs, imprimantes ou autres appareils sur un réseau. Il faut faire la distinction entre adresse IP globale et privée. Les adresses IP globales sont souvent données de manière dynamique par les fournisseurs d'accès à Internet (voir DHCP). Elles rendent votre réseau local, ou un ordinateur seul, accessible depuis Internet. Les adresses IP privées sont données de manière dynamique (DHCP) ou statique (attribuée „à la main") par l'utilisateur. Les adresses IP assignent un appareil à un réseau précis.

  EXEMPLE :
  Les adresses IP sont le type d'adressage le plus courant sur le réseau et ont par exemple la forme suivante : 192.168.0.1

- **Adresse MAC**
  L'adresse MAC désigne l'adresse physique d'un composant réseau (p.ex carte réseau, dongle WiFi, imprimante, switch). Les adresses MAC restent les mêmes pour un même appareil contrairement aux adresses IP qui peuvent varier. Les adresses MAC des appareils réseau connectés sont enregistrées dans un tableau dit

ARP. Les tableaux ARP peuvent permettre de dépanner un appareil du réseau qui ne dispose pas d'adresse IP (p.ex. switch).

EXEMPLE :
Une adresse MAC ressemble à cela : 00:00:C0:5A:42:C1

- **Blacklist (liste noire)**
  Une Blacklist en réseau est une liste de périphériques dont la connexion est refusée (par exemple à un routeur). Tous les autres appareils sont acceptées par le dispositif qui réglemente l'accès via la Blacklist. Il existe aussi une liste inverse nommée Whitelist (liste blanche).

- **Browser (Navigateur)**
  Un Browser est un programme qui permet de naviguer sur Internet. Les navigateurs les plus connus sont Internet Explorer, Mozilla Firefox, Opera et Google Chrome.

- **Client**
  Un Client est une application qui prend en compte les données d'un service serveur. Une connexion classique Client-Serveur est souvent présente dans les réseaux domestiques lors de l'assignation automatique des adresses IP. L'ordinateur est alors un client DHCP qui demande une adresse IP valide à un serveur DHCP (souvent le routeur) qui les distribue.

- **Cryptage**
  Les techniques de cryptage sont utilisées dans des réseaux pour protéger vos données contre les accès non autorisés. Ces mécanismes de cryptage fonctionnent de manière similaire à une carte de crédit. C'est seulement avec le bon mot de passe (code PIN) que les données peuvent être décryptées.

- **Espace d'adresses**
  Une plage d'adresses est un groupe défini d'adresses IP ou MAC rassemblées en une même „unité de gestion".

- **ISP (FAI)**
  ISP est l'abréviation de „Internet Service Provider", soit „Fournisseur d'Accès à Internet" (FAI). Ce terme est utilisé pour les entreprises qui proposent un moyen d'accès au réseau Internet. En France, les FAI les plus connus sont Orange, Free, Bouygues et Neuf-SFR.

- **LAN**
  LAN (Local Area Network) décrit un réseau d'ordinateurs et autres appareils en réseau qui disposent d'un adressage commun qui les regroupe dans une même structure.

- **Mots de passe sécurisés**
  Un mot de passe sécurisé désigne un mot de passe qui remplit certaines conditions afin de ne pas être décrypté facilement en cas d'attaque pirate.
  Le mot de passe sécurisé a généralement une longueur minimale et contient plusieurs caractères spéciaux. Une règle de base s'applique ici: plus le mot de passe est long et plus il contient de caractères spéciaux, plus il est sécurisé contre le décryptage.

- **Passphrase (phrase de passe)**
  Une Passphrase désigne un ou plusieurs mots-clés qui servent de question de sécurité ; ils doivent être saisis avant la connexion à un réseau crypté WPA / WPA2 .

- **Port**
  Le port est une connexion logicielle qui permet la communication entre des applications de votre ordinateur et des applications tierces. Il faut distinguer ici deux protocoles : TCP et UDP.

  EXEMPLE :
  L'application principale pour Internet est un navigateur (Internet Explorer, Mozilla Firefox, etc.) utilisant principalement le port TCP 80 pour communiquer avec les serveurs des hébergeurs de pages web.

- **Pre-Shared Key (Clé pré-partagée)**
  Pre-Shared Key („Clé pré-partagée“) aussi abrégé en PSK, décrit un type de cryptage qui oblige les deux partis à connaître la clé avant de pour se connecter (voir aussi WPA/WPA2).

- **Protocole**
  Les protocoles en réseau sont des standards pour les paquets de données que les appareils s'échangent afin de permettre une communication claire.

- **Sous-réseau**
  Les sous-réseaux sont un regroupement d'adresses IP en structure réseau. Ceci permet de regrouper les ordinateurs de chaque bureau dans un sous-réseau distinct. Les sous-réseaux sont donc une structure utile. Une saisie du sous-réseau va de pair avec celle d'une adresse IP. Dans un réseau local, il n'est normalement pas utile de configurer des sous-réseaux. C'est pourquoi le sous-réseau Windows par défaut est 255.255.255.0. Vous disposez ainsi des adresses IP xxx.xxx.xxx.1 à xxx.xxx.xxx.254.

- **SSID**
  SSID (Service Set Identifier) permet de définir un réseau sans fil (Wi-Fi). Ce SSID est souvent diffusé (voir UDP) publiquement afin de rendre le réseau visible par les appareils mobiles qui voudraient s'y connecter.

- **TCP (Transmission Control Protocol)**
  Le protocole TCP est utilisé pour demander des informations précises à un correspondant distant (voir Port).

- **UDP (User Datagram Protocol)**
  Le protocole UDP est un protocole dit „Broadcast'. Broadcast est aussi utilisé en anglais pour décrire les diffuseurs Radio ou TV. Ce protocole fonctionne de manière similaire. Il est utilisé pour envoyer des paquets de données dans tous les réseaux accessibles et attend ensuite le retour de ces appareils. Le protocole UDP est surtout utilisé pour les applications quand il n'est pas certain qu'un récepteur correspondant est disponible sur le réseau.

- **uPNP**
  Cet acronyme décrit le protocole „Universal Plug and Play". Ce protocole est principalement utilisé pour gérer les imprimantes et autres périphériques similaires via un réseau.

- **VPN**
  VPN (Virtual Private Network) désigne une interface réseau qui permet de connecter des appareils à un réseau voisin sans que ce dernier soit compatible.

- **WAN**
  WAN (Wide Area Network) décrit un réseau d'ordinateurs et autres appareils en réseau qui regroupe plusieurs composants distants. L'exemple le plus connu est „Internet". Un WAN peut aussi se composer uniquement de deux réseaux LAN .

- **Whitelist (liste blanche)**
  Une Whitelist en réseau est une liste d'appareil dont la connexion est acceptée explicitement (par exemple à un routeur). Tous les autres appareils sont refusés par le dispositif qui réglemente l'accès via la Whitelist. Il existe aussi une liste inverse nommée Blacklist.

Services réseau

- **Adresse statique**
  L'assignation d'adresse IP statique s'oppose à l'assignation dynamique DHCP et toutes les adresses d'un réseau restent fixes. Chaque Client (ordinateur) du réseau dispose de sa propre adresse IP, masque sous-réseau, passerelle standard et serveur DNS fixe. Il doit se présenter au serveur avec ces données.
  Un nouveau Client (ordinateur) doit d'abord être configuré avec une adresse IP valide et encore disponible avant de pouvoir utiliser le réseau. L'assignation d'adresse IP manuelle est utile pour les imprimantes réseau ou autres appareils auxquels on accède souvent, ou dans des réseaux particulièrement sécurisés.

- **DHCP (Dynamic Host Configuration Protocol)**
  Le DHCP est l'assignation automatique des adresses IP dans le réseau. Ces adresses sont dites dynamiques car elles peuvent être modifiées facilement et à tout moment. Les adresses IP dynamiques peuvent être décrites comme des adresses IP louées. Ces adresses IP louées contiennent une „Date de péremption" aussi appelé „Lease Time". Un ordinateur demandera une nouvelle adresse IP au serveur DHCP une fois que le „Lease" est écoulé. Ceci est cependant une source d'erreur car il peut survenir des incohérences entre serveur DHCP et Clients DHCP.

NOTE :
Les ordinateurs Windows sont configurés par défaut comme clients DHCP pour permettre un branchement simple au réseau domestique.

- **DNS (Domain Name Server)**
  DNS est un service réseau qui traduit les adresses IP en adresses Internet. L'adresse www.google.de est en réalité l'adresse IP: 74.125.39.105. Si vous devez saisir une adresse DNS-IP pendant une configuration, saisissez l'adresse du serveur DNS. Pour des raisons de sécurité contre les pannes, les serveurs DNS fonctionnent souvent par paires et sont nommés DNS primaire (ou DNS1) et DNS secondaire (ou DNS2).

- **Filtre**
  Voir aussi Firewall

- **Firewall (pare-feu)**
  Un Firewall ou pare-feu est un mécanisme de sécurité qui fonctionne souvent sur les routeurs comme un service réseau mais qui est également intégré dans Windows (depuis XP). Il permet l'accès via certains ports, bloque les adresses IP configurées précédemment et évite les accès dangereux à votre réseau.

- **FTP/NAS (File Transfer Protocol/ Network Access Storage)**
  FTP est un service serveur qui est principalement utilisé pour transférer des fichiers. Ce service permet de transférer facilement des fichiers d'un ordinateur à un autre via une interface similaire à l'explorateur Windows. Les serveurs NAS proposent aussi ce service pour permettre l'accès à un disque dur sur l'ensemble du réseau.

- **HTTP/Webserver (Hypertext Transfer Protocol)**
  Ce service est aussi couramment appelé „Internet". Mais il s'agit d'une vulgarisation car l'Internet en soi est une structure supérieure qui contient presque tous les services réseau. HTTP est utilisé pour le transfert et l'affichage de pages web.

- **Mediastreams (flux média)**
  Ce groupe de services réseau est utilisé par de nombreux appareils et fournisseurs. Les exemples les plus connus sont les webradios, la Video-On-Demand et les caméras IP. Ces flux en direct utilisent différents protocoles et versions. C'est pourquoi il peut survenir des incompatibilités entre serveur et client.

- **NTP**
  NTP (Network Time Protcol) désigne un protocole qui permet de régler la date et l'heure de l'ordinateur via le réseau. Ce service est fourni par des serveurs répartis dans le monde entier.

- **Passerelle (standard)**
  La passerelle est la connectique qui permet la communication entre les ordinateurs du réseau local et les ordinateurs de l'extérieur. Elle va de pair avec votre routeur . La passerelle rassemble les demandes des Clients et les transfère aux serveurs correspondants sur Internet. La passerelle distribue aussi les réponses des serveurs aux Clients qui avaient fait la demande.

- **PPPoE**
  PPPoE signifie PPP over Ethernet et désigne un protocole réseau Point-to-Point Protocol (PPP) via une connexion Ethernet. PPPoE est souvent utilisé en France avec les connexions ADSL. ADSL signifie DSL Asynchrone et désigne l'utilisation d'une même ligne pour le téléphone et Internet. ADSL est le standard en France. La raison principale pour l'utilisation du PPPoE est la possibilité de rendre disponible l'authentification et la configuration réseau (adresse IP, passerelle) sur le rapide réseau Ethernet.

- **Samba/SMB**
  Cela désigne un service de serveur utilisé spécialement sur les réseaux Windows. Ce service permet également un accès rapide et facile aux données stockées sur d'autres ordinateurs (dans les „dossiers partagés"). Toutefois, ce service est limité aux réseaux domestiques, et n'est pas conçu pour être contrôlé via Internet.

- **Serveur/Service serveur**
  Un serveur est une sorte de prestataire de services en réseau. Des applications simples sont aussi dénommées services serveur. Les plus connus sont entre autre Webserver, DHCP ou serveur E-Mail. Plusieurs de ces services peuvent être disponibles simultanément sur un ordinateur ou d'autres appareil (p.ex. routeurs). Les serveurs sont aussi appelés ordinateurs car leur fonction unique est de fournir et de gérer des services réseau.

- **WEP et WPA**
  Wired Equivalent Privacy (WEP) est l'algorithme de cryptage standard pour les anciens réseaux Wi-Fi. Il réglemente l'accès au réseau et assure la confidentialité des données. Les nombreuses faiblesses de cet algorithme en font un cryptage qui n'est plus sécurisé. C'est pourquoi les installations Wi-Fi devraient utiliser un cryptage WPA plus sûr. Wi-Fi Protected Access (WPA) est l'algorithme de cryptage pour un réseau Wi-Fi. Il est l'évolution du WEP et est plus sécurisé.

MESURES DE SÉCURITÉ DANS LES RÉSEAUX WI-FI

En premier lieu, ne pas utiliser le WEP, mais préférer le cryptage WPA ou WPA2. Cet objectif est souvent atteint par une simple mise à jour des pilotes ou du firmware. Si vous êtes obligé d'utiliser le WEP, certaines mesures doivent être prises pour minimiser le risque d'accès indésirable au réseau Wi-Fi :

- Activez toujours la protection par mot de passe ! Modifiez éventuellement le mot de passe de votre routeur ou point d'accès.
- Si vous utilisez le cryptage WEP parce qu'un des périphériques connecté ne supporte pas le WPA ni le WPA2 (cryptages recommandés), utilisez alors une clé WEP de 128 bits minimum, avec lettres, chiffres et caractères spéciaux en ordre aléatoire.
- Activez la liste de contrôle d'accès (ACL = Access Control List) pour que le routeur accepte uniquement des périphériques avec adresse MAC connue. Notez qu'une adresse MAC est facilement modifiable par logiciel, de sorte qu'une adresse MAC acceptée peut être réassignée par n'importe qui.
- Utilisez un SSID anonyme : le SSID du routeur (ou Access-Point) ne doit pas contenir votre nom et ne doit ni permettre d'identifier votre matériel et/ou emplacement d'utilisation.
- La désactivation de la publication du SSID (Broadcasting) est sujette à controverse. Elle empêche une connexion accidentelle au réseau Wi-Fi, mais un SSID caché restera tout de même détectable avec des logiciels dits „sniffer".
- Il est préférable de configurer les périphériques Wi-Fi (tout comme le point d'accès) avec une connexion filaire.
- Éteignez les périphériques Wi-Fi quand ils ne sont pas utilisés.
- Procédez régulièrement à des mises à jour du firmware du point d'accès afin d'obtenir les mises à jour de sécurité.
- Vous pouvez maîtriser la portée du réseau sans fil en réduisant la puissance d'envoi ou en choisissant l'emplacement du périphérique sans fil (ceci n'est pas une mesure de sécurité active mais limite seulement le rayon d'attaque possible).

Toutes ces mesures de sécurité restent quasiment inutiles en cas d'utilisation d'un cryptage WEP. Avec les bons outils et connaissances techniques, un cryptage WEP peut être piraté aisément, en 5 à 10 minutes.

CONTRAT DE LICENCE DE LOGICIEL LIBRE CECILL

Ce produit contient un logiciel distribué entièrement ou partiellement sous licence publique générale GNU, Version 2 (GPL).
Vous trouverez ci-après l'intégralité de la version actuelle de ce texte de licence.
Puisqu'il s'agit d'un logiciel libre de droits, ses développeurs déclinent toute responsabilité en cas de dégâts ou dommages (physiques ou moraux) dus à une mauvaise utilisation.
Veuillez noter que la garantie du matériel n'est bien entendu pas concernée. Si vous avez des questions, n'hésitez pas à nous contacter. Pour cela, rendez-vous sur HYPERLINK "http://www.pearl.fr/"www.pearl.fr.

Avertissement

Ce contrat est une licence de logiciel libre issue d'une concertation entre ses auteurs afin que le respect de deux grands principes préside à sa rédaction:

* d'une part, le respect des principes de diffusion des logiciels libres: accès au code source, droits étendus conférés aux utilisateurs,
* d'autre part, la désignation d'un droit applicable, le droit français, auquel elle est conforme, tant au regard du droit de la responsabilité civile que du droit de la propriété intellectuelle et de la protection qu'il offre aux auteurs et titulaires des droits patrimoniaux sur un logiciel.

Les auteurs de la licence CeCILL (pour Ce[a] C[nrs] l[nria] L[ogiciel] L[ibre]) sont:

Commissariat à l'Énergie Atomique - CEA, établissement public de recherche à caractère scientifique, technique et industriel, dont le siège est situé 25 rue Leblanc, immeuble Le Ponant D, 75015 Paris.

Centre National de la Recherche Scientifique - CNRS, établissement public à caractère scientifique et technologique, dont le siège est situé 3 rue Michel-Ange, 75794 Paris cedex 16.

Institut National de Recherche en Informatique et en Automatique - INRIA, établissement public à caractère scientifique et technologique, dont le siège est situé Domaine de Voluceau, Rocquencourt, BP 105, 78153 Le Chesnay cedex.

Préambule

Ce contrat est une licence de logiciel libre dont l'objectif est de conférer aux utilisateurs la liberté de modification et de redistribution du logiciel régi par cette licence dans le cadre d'un modèle de diffusion en logiciel libre.

L'exercice de ces libertés est assorti de certains devoirs à la charge des utilisateurs afin de préserver ce statut au cours des redistributions ultérieures.

L'accessibilité au code source et les droits de copie, de modification et de redistribution qui en découlent ont pour contrepartie de n'offrir aux utilisateurs qu'une garantie limitée et de ne faire peser sur l'auteur du logiciel, le titulaire des droits patrimoniaux et les concédants successifs qu'une responsabilité restreinte.

A cet égard l'attention de l'utilisateur est attirée sur les risques associés au chargement, à l'utilisation, à la modification et/ou au développement et à la reproduction du logiciel par l'utilisateur étant donné sa spécificité de logiciel libre, qui peut le rendre complexe à manipuler et qui le réserve donc à des développeurs ou des professionnels avertis possédant des connaissances informatiques approfondies. Les utilisateurs sont donc invités à charger et tester l'adéquation du logiciel à leurs besoins dans des conditions permettant d'assurer la sécurité de leurs systèmes et/ou de leurs données et, plus généralement, à l'utiliser et l'exploiter dans les mêmes conditions de sécurité. Ce contrat peut être reproduit et diffusé librement, sous réserve de le conserver en l'état, sans ajout ni suppression de clauses.

Ce contrat est susceptible de s'appliquer à tout logiciel dont le titulaire des droits patrimoniaux décide de soumettre l'exploitation aux dispositions qu'il contient.

Article 1 - DÉFINITIONS

Dans ce contrat, les termes suivants, lorsqu'ils seront écrits avec une lettre capitale, auront la signification suivante:

Contrat: désigne le présent contrat de licence, ses éventuelles versions postérieures et annexes.

Logiciel: désigne le logiciel sous sa forme de Code Objet et/ou de Code Source et le cas échéant sa documentation, dans leur état au moment de l'acceptation du Contrat par le Licencié.

Logiciel Initial: désigne le Logiciel sous sa forme de Code Source et éventuellement de Code Objet et le cas échéant sa documentation, dans leur état au moment de leur première diffusion sous les termes du Contrat.

Logiciel Modifié: désigne le Logiciel modifié par au moins une Contribution.

Code Source: désigne l'ensemble des instructions et des lignes de programme du Logiciel et auquel l'accès est nécessaire en vue de modifier le Logiciel.

Code Objet: désigne les fichiers binaires issus de la compilation du Code Source.

Titulaire: désigne le ou les détenteurs des droits patrimoniaux d'auteur sur le Logiciel Initial.

Licencié: désigne le ou les utilisateurs du Logiciel ayant accepté le Contrat.

Contributeur: désigne le Licencié auteur d'au moins une Contribution.

Concédant: désigne le Titulaire ou toute personne physique ou morale distribuant le Logiciel sous le Contrat.

Contribution: désigne l'ensemble des modifications, corrections, traductions, adaptations et/ou nouvelles fonctionnalités intégrées dans le Logiciel par tout Contributeur, ainsi que tout Module Interne.

Module: désigne un ensemble de fichiers sources y compris leur documentation qui permet de réaliser des fonctionnalités ou services supplémentaires à ceux fournis par le Logiciel.

Module Externe: désigne tout Module, non dérivé du Logiciel, tel que ce Module et le Logiciel s'exécutent dans des espaces d'adressage différents, l'un appelant l'autre au moment de leur exécution.

Module Interne: désigne tout Module lié au Logiciel de telle sorte qu'ils s'exécutent dans le même espace d'adressage.

GNU GPL: désigne la GNU General Public License dans sa version 2 ou toute version ultérieure, telle que publiée par Free Software Foundation Inc.

Parties: désigne collectivement le Licencié et le Concédant.

Ces termes s'entendent au singulier comme au pluriel.

Article 2 - OBJET

Le Contrat a pour objet la concession par le Concédant au Licencié d'une licence non exclusive, cessible et mondiale du Logiciel telle que définie ci-après à l'article 5 pour toute la durée de protection des droits portant sur ce Logiciel.

Article 3 - ACCEPTATION

3.1 L'acceptation par le Licencié des termes du Contrat est réputée acquise du fait du premier des faits suivants:

* (I) le chargement du Logiciel par tout moyen notamment par téléchargement à partir d'un serveur distant ou par chargement à partir d'un support physique;
* (II) le premier exercice par le Licencié de l'un quelconque des droits concédés par le Contrat.

3.2 Un exemplaire du Contrat, contenant notamment un avertissement relatif aux spécificités du Logiciel, à la restriction de garantie et à la limitation à un usage par des utilisateurs expérimentés a été mis à disposition du Licencié préalablement à son acceptation telle que définie à l'article 3.1 ci dessus et le Licencié reconnaît en avoir pris connaissance.

Article 4 - ENTRÉE EN VIGUEUR ET DURÉE

4.1 ENTRÉE EN VIGUEUR

Le Contrat entre en vigueur à la date de son acceptation par le Licencié telle que définie en 3.1.

4.2 DURÉE

Le Contrat produira ses effets pendant toute la durée légale de protection des droits patrimoniaux portant sur le Logiciel.

Article 5 - ÉTENDUE DES DROITS CONCÉDÉS

Le Concédant concède au Licencié, qui accepte, les droits suivants sur le Logiciel pour toutes destinations et pour la durée du Contrat dans les conditions ci-après détaillées.

Par ailleurs, si le Concédant détient ou venait à détenir un ou plusieurs brevets d'invention protégeant tout ou partie des fonctionnalités du Logiciel ou de ses composants, il s'engage à ne pas opposer les éventuels droits conférés par ces brevets aux Licenciés successifs qui utiliseraient, exploiteraient ou modifieraient le Logiciel. En cas de cession de ces brevets, le Concédant s'engage à faire reprendre les obligations du présent alinéa aux cessionnaires.

5.1 DROIT D'UTILISATION

Le Licencié est autorisé à utiliser le Logiciel, sans restriction quant aux domaines d'application, étant ci-après précisé que cela comporte:

1. la reproduction permanente ou provisoire du Logiciel en tout ou partie par tout moyen et sous toute forme.

2. le chargement, l'affichage, l'exécution, ou le stockage du Logiciel sur tout support.

3. la possibilité d'en observer, d'en étudier, ou d'en tester le fonctionnement afin de déterminer les idées et principes qui sont à la base de n'importe quel élément de ce Logiciel; et ceci, lorsque le Licencié effectue toute opération de chargement, d'affichage, d'exécution, de transmission ou de stockage du Logiciel qu'il est en droit d'effectuer en vertu du Contrat.

5.2 DROIT D'APPORTER DES CONTRIBUTIONS

Le droit d'apporter des Contributions comporte le droit de traduire, d'adapter, d'arranger ou d'apporter toute autre modification au Logiciel et le droit de reproduire le logiciel en résultant.

Le Licencié est autorisé à apporter toute Contribution au Logiciel sous réserve de mentionner, de façon explicite, son nom en tant qu'auteur de cette Contribution et la date de création de celle-ci.

5.3 DROIT DE DISTRIBUTION

Le droit de distribution comporte notamment le droit de diffuser, de transmettre et de communiquer le Logiciel au public sur tout support et par tout moyen ainsi que le droit de mettre sur le marché à titre onéreux ou gratuit, un ou des exemplaires du Logiciel par tout procédé.

Le Licencié est autorisé à distribuer des copies du Logiciel, modifié ou non, à des tiers dans les conditions ci-après détaillées.

5.3.1 DISTRIBUTION DU LOGICIEL SANS MODIFICATION

Le Licencié est autorisé à distribuer des copies conformes du Logiciel, sous forme de Code Source ou de Code Objet, à condition que cette distribution respecte les dispositions du Contrat dans leur totalité et soit accompagnée:

1. d'un exemplaire du Contrat,

2. d'un avertissement relatif à la restriction de garantie et de responsabilité du Concédant telle que prévue aux articles 8 et 9,et que, dans le cas où seul le Code Objet du Logiciel est redistribué, le Licencié permette aux futurs Licenciés d'accéder facilement au Code Source complet du Logiciel en indiquant les modalités d'accès, étant entendu que le coût additionnel d'acquisition du Code Source ne devra pas excéder le simple coût de transfert des données.

5.3.2 DISTRIBUTION DU LOGICIEL MODIFIÉ

Lorsque le Licencié apporte une Contribution au Logiciel, les conditions de distribution du Logiciel Modifié en résultant sont alors soumises à l'intégralité des dispositions du Contrat.

Le Licencié est autorisé à distribuer le Logiciel Modifié, sous forme de code source ou de code objet, à condition que cette distribution respecte les dispositions du Contrat dans leur totalité et soit accompagnée:

1. d'un exemplaire du Contrat,

2. d'un avertissement relatif à la restriction de garantie et de responsabilité du Concédant telle que prévue aux articles 8 et 9,et que, dans le cas où seul le code objet du Logiciel Modifié est redistribué, le Licencié permette aux futurs Licenciés d'accéder facilement au code source complet du Logiciel Modifié en indiquant les modalités d'accès, étant entendu que le coût additionnel d'acquisition du code source ne devra pas excéder le simple coût de transfert des données.

5.3.3 DISTRIBUTION DES MODULES EXTERNES

Lorsque le Licencié a développé un Module Externe les conditions du Contrat ne s'appliquent pas à ce Module Externe, qui peut être distribué sous un contrat de licence différent.

5.3.4 COMPATIBILITÉ AVEC LA LICENCE GNU GPL

Le Licencié peut inclure un code soumis aux dispositions d'une des versions de la licence GNU GPL dans le Logiciel modifié ou non et distribuer l'ensemble sous les conditions de la même version de la licence GNU GPL.

Le Licencié peut inclure le Logiciel modifié ou non dans un code soumis aux dispositions d'une des versions de la licence GNU GPL et distribuer l'ensemble sous les conditions de la même version de la licence GNU GPL.

Article 6 - PROPRIÉTÉ INTELLECTUELLE

6.1 SUR LE LOGICIEL INITIAL

Le Titulaire est détenteur des droits patrimoniaux sur le Logiciel Initial. Toute utilisation du Logiciel Initial est soumise au respect des conditions dans lesquelles le Titulaire a choisi de diffuser son œuvre et nul autre n'a la faculté de modifier les conditions de diffusion de ce Logiciel Initial.

Le Titulaire s'engage à ce que le Logiciel Initial reste au moins régi par le Contrat et ce, pour la durée visée à l'article 4.2.

6.2 SUR LES CONTRIBUTIONS

Le Licencié qui a développé une Contribution est titulaire sur celle-ci des droits de propriété intellectuelle dans les conditions définies par la législation applicable.

6.3 SUR LES MODULES EXTERNES

Le Licencié qui a développé un Module Externe est titulaire sur celui-ci des droits de propriété intellectuelle dans les conditions définies par la législation applicable et reste libre du choix du contrat régissant sa diffusion.

6.4 DISPOSITIONS COMMUNES

Le Licencié s'engage expressément:

1. à ne pas supprimer ou modifier de quelque manière que ce soit les mentions de propriété intellectuelle apposées sur le Logiciel;

2. à reproduire à l'identique lesdites mentions de propriété intellectuelle sur les copies du Logiciel modifié ou non.

Le Licencié s'engage à ne pas porter atteinte, directement ou indirectement, aux droits de propriété intellectuelle du Titulaire et/ou des Contributeurs sur le Logiciel et à prendre, le cas échéant, à l'égard de son personnel toutes les mesures nécessaires pour assurer le respect des dits droits de propriété intellectuelle du Titulaire et/ou des Contributeurs.

Article 7 - SERVICES ASSOCIÉS

7.1 Le Contrat n'oblige en aucun cas le Concédant à la réalisation de prestations d'assistance technique ou de maintenance du Logiciel.

Cependant le Concédant reste libre de proposer ce type de services. Les termes et conditions d'une telle assistance technique et/ou d'une telle maintenance seront alors déterminés dans un acte séparé. Ces actes de maintenance et/ou assistance technique n'engageront que la seule responsabilité du Concédant qui les propose.

7.2 De même, tout Concédant est libre de proposer, sous sa seule responsabilité, à ses licenciés une garantie, qui n'engagera que lui, lors de la redistribution du Logiciel et/ou du Logiciel Modifié et ce, dans les conditions qu'il souhaite. Cette garantie et

les modalités financières de son application feront l'objet d'un acte séparé entre le Concédant et le Licencié.

Article 8 - RESPONSABILITÉ

8.1 Sous réserve des dispositions de l'article 8.2, le Licencié a la faculté, sous réserve de prouver la faute du Concédant concerné, de solliciter la réparation du préjudice direct qu'il subirait du fait du Logiciel et dont il apportera la preuve.

8.2 La responsabilité du Concédant est limitée aux engagements pris en application du Contrat et ne saurait être engagée en raison notamment:
(I) des dommages dus à l'inexécution, totale ou partielle, de ses obligations par le Licencié, (II) des dommages directs ou indirects découlant de l'utilisation ou des performances du Logiciel subis par le Licencié et (III) plus généralement d'un quelconque dommage indirect. En particulier, les Parties conviennent expressément que tout préjudice financier ou commercial (par exemple perte de données, perte de bénéfices, perte d'exploitation, perte de clientèle ou de commandes, manque à gagner, trouble commercial quelconque) ou toute action dirigée contre le Licencié par un tiers, constitue un dommage indirect et n'ouvre pas droit à réparation par le Concédant.

Article 9 - GARANTIE

9.1 Le Licencié reconnaît que l'état actuel des connaissances scientifiques et techniques au moment de la mise en circulation du Logiciel ne permet pas d'en tester et d'en vérifier toutes les utilisations ni de détecter l'existence d'éventuels défauts. L'attention du Licencié a été attirée sur ce point sur les risques associés au chargement, à l'utilisation, la modification et/ou au développement et à la reproduction du Logiciel qui sont réservés à des utilisateurs avertis.

Il relève de la responsabilité du Licencié de contrôler, par tous moyens, l'adéquation du produit à ses besoins, son bon fonctionnement et de s'assurer qu'il ne causera pas de dommages aux personnes et aux biens.

9.2 Le Concédant déclare de bonne foi être en droit de concéder l'ensemble des droits attachés au Logiciel (comprenant notamment les droits visés à l'article 5).

9.3 Le Licencié reconnaît que le Logiciel est fourni "en l'état" par le Concédant sans autre garantie, expresse ou tacite, que celle prévue à l'article 9.2 et notamment sans aucune garantie sur sa valeur commerciale, son caractère sécurisé, innovant ou pertinent.

En particulier, le Concédant ne garantit pas que le Logiciel est exempt d'erreur, qu'il fonctionnera sans interruption, qu'il sera compatible avec l'équipement du Licencié et sa configuration logicielle ni qu'il remplira les besoins du Licencié.

9.4 Le Concédant ne garantit pas, de manière expresse ou tacite, que le Logiciel ne porte pas atteinte à un quelconque droit de propriété intellectuelle d'un tiers portant sur un brevet, un logiciel ou sur tout autre droit de propriété. Ainsi, le Concédant exclut toute garantie au profit du Licencié contre les actions en contrefaçon qui pourraient être diligentées au titre de l'utilisation, de la modification, et de la redistribution du Logiciel. Néanmoins, si de telles actions sont exercées contre le Licencié, le Concédant lui apportera son aide technique et juridique pour sa défense. Cette aide technique

et juridique est déterminée au cas par cas entre le Concédant concerné et le Licencié dans le cadre d'un protocole d'accord. Le Concédant dégage toute responsabilité quant à l'utilisation de la dénomination du Logiciel par le Licencié. Aucune garantie n'est apportée quant à l'existence de droits antérieurs sur le nom du Logiciel et sur l'existence d'une marque.

Article 10 - RÉSILIATION

10.1 En cas de manquement par le Licencié aux obligations mises à sa charge par le Contrat, le Concédant pourra résilier de plein droit le Contrat trente (30) jours après notification adressée au Licencié et restée sans effet.

10.2 Le Licencié dont le Contrat est résilié n'est plus autorisé à utiliser, modifier ou distribuer le Logiciel. Cependant, toutes les licences qu'il aura concédées antérieurement à la résiliation du Contrat resteront valides sous réserve qu'elles aient été effectuées en conformité avec le Contrat.

Article 11 - DISPOSITIONS DIVERSES

11.1 CAUSE EXTÉRIEURE

Aucune des Parties ne sera responsable d'un retard ou d'une défaillance d'exécution du Contrat qui serait dû à un cas de force majeure, un cas fortuit ou une cause extérieure, telle que, notamment, le mauvais fonctionnement ou les interruptions du réseau électrique ou de télécommunication, la paralysie du réseau liée à une attaque informatique, l'intervention des autorités gouvernementales, les catastrophes naturelles, les dégâts des eaux, les tremblements de terre, le feu, les explosions, les grèves et les conflits sociaux, l'état de guerre...

11.2 Le fait, par l'une ou l'autre des Parties, d'omettre en une ou plusieurs occasions de se prévaloir d'une ou plusieurs dispositions du Contrat, ne pourra en aucun cas impliquer renonciation par la Partie intéressée à s'en prévaloir ultérieurement.

11.3 Le Contrat annule et remplace toute convention antérieure, écrite ou orale, entre les Parties sur le même objet et constitue l'accord entier entre les Parties sur cet objet. Aucune addition ou modification aux termes du Contrat n'aura d'effet à l'égard des Parties à moins d'être faite par écrit et signée par leurs représentants dûment habilités.

11.4 Dans l'hypothèse où une ou plusieurs des dispositions du Contrat s'avèrerait contraire à une loi ou à un texte applicable, existants ou futurs, cette loi ou ce texte prévaudrait, et les Parties feraient les amendements nécessaires pour se conformer à cette loi ou à ce texte. Toutes les autres dispositions resteront en vigueur. De même, la nullité, pour quelque raison que ce soit, d'une des dispositions du Contrat ne saurait entraîner la nullité de l'ensemble du Contrat.

11.5 LANGUE

Le Contrat est rédigé en langue française et en langue anglaise, ces deux versions faisant également foi.

Article 12 - NOUVELLES VERSIONS DU CONTRAT

12.1 Toute personne est autorisée à copier et distribuer des copies de ce Contrat.

12.2 Afin d'en préserver la cohérence, le texte du Contrat est protégé et ne peut être modifié que par les auteurs de la licence, lesquels se réservent le droit de publier périodiquement des mises à jour ou de nouvelles versions du Contrat, qui posséderont chacune un numéro distinct. Ces versions ultérieures seront susceptibles de prendre en compte de nouvelles problématiques rencontrées par les logiciels libres.

12.3 Tout Logiciel diffusé sous une version donnée du Contrat ne pourra faire l'objet d'une diffusion ultérieure que sous la même version du Contrat ou une version postérieure, sous réserve des dispositions de l'article 5.3.4.

Article 13 - LOI APPLICABLE ET COMPÉTENCE TERRITORIALE

13.1 Le Contrat est régi par la loi française. Les Parties conviennent de tenter de régler à l'amiable les différends ou litiges qui viendraient à se produire par suite ou à l'occasion du Contrat.

13.2 A défaut d'accord amiable dans un délai de deux (2) mois à compter de leur survenance et sauf situation relevant d'une procédure d'urgence, les différends ou litiges seront portés par la Partie la plus diligente devant les Tribunaux compétents de Paris.

Version 2.0 du 2006-09-05.